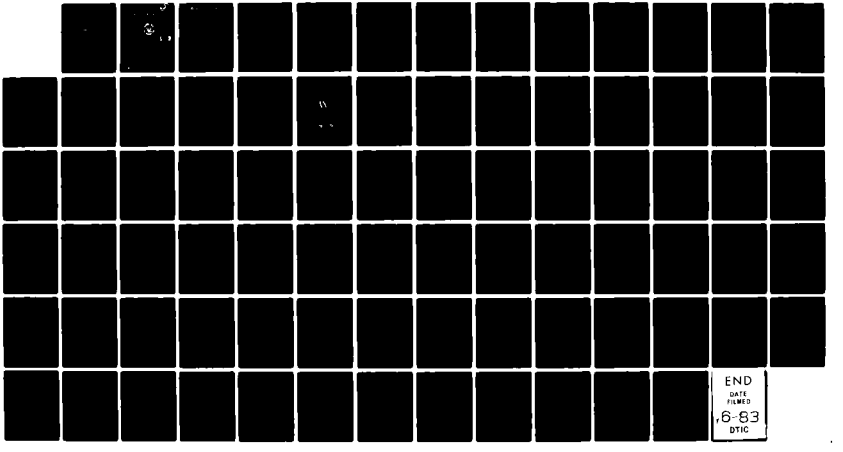
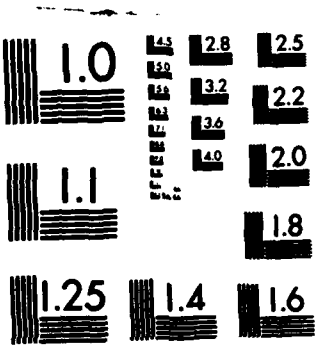
AD-A128 127 IMPACT OF THE WIS MODERNIZATION PLAN ON THE JOINT DEPLOYMENT SYSTEM(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA M MCLENDON-KOENIG MAR 83 1/1

UNCLASSIFIED F/G 9/2 NL



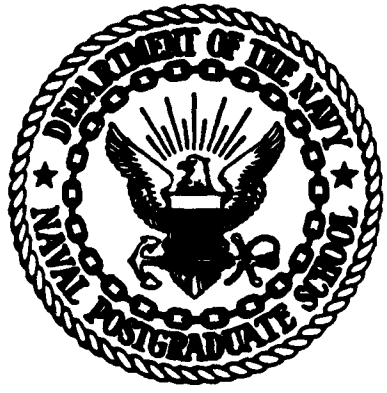
END
DATE FILMED
6-83
DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AD A128127

NAVAL POSTGRADUATE SCHOOL
Monterey, California



DTIC
ELECTE
MAY 17 1983
S D
D

THESIS

IMPACT OF THE WIS MODERNIZATION PLAN
ON THE JOINT DEPLOYMENT SYSTEM

by

Mary McLendon-Koenig

March 1983

Thesis Advisor: L. B. Garden

Approved for public release; distribution unlimited.

DTIC FILE COPY

83 05 16 134

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A128127	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Impact of the WIS Modernization Plan on the Joint Deployment System	5. TYPE OF REPORT & PERIOD COVERED Master's Thesis; March 1983
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Mary McLendon-Koenig	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940	12. REPORT DATE March 1983
	13. NUMBER OF PAGES 79
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)	15. SECURITY CLASS. (of this report) Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

WWMCCS Information System (WIS), Defense Data Network (DDN), Joint Deployment System (JDS), WWMCCS Intercomputer Network (WIN), Remote User's Package (RUP), IVY LEAGUE 82, JDS Interface Processor (JDSIP), JDS Update Processor (JDSUP)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Joint Deployment System (JDS) forms the junction among deliberate planning, time-sensitive planning, and the deployment of forces. The WWMCCS Intercomputer Network (WIN) supplies the necessary interconnectivity among the joint deployment community computer systems. In January 1982, the WWMCCS Information System (WIS) modernization program was launched with objectives including the modernization of WWMCCS hardware and software and the transfer from the present WWMCCS network system to the Defense Data

Cont'd

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE S/N 0102-LF-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Network (DDN). Because of proven WIN unreliability, the JOS required site-unique software development to supplement present WIN software.

Individualized application software, integrated with the improved network reliability and survivability of the DDN, will enhance the present C3 system. This thesis demonstrates that the total implementation of the WIS involves additional modifications in site-unique applications, standardized procedures for software development, updated hardware technology, and a multi-level security system.

Accession For	
NTIS GRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A	

Approved for public release; distribution unlimited

Impact of the WIS Modernization Plan on the Joint Deployment System

by

Mary McLendon-Koenig
Lieutenant, United States Navy
B.S., Armstrong State College, 1978

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(COMMAND, CONTROL AND COMMUNICATIONS)

from the

NAVAL POSTGRADUATE SCHOOL
March 1983

Author: Mary McLendon-Koenig

Approved by: Leo B Bauden
Thesis Advisor

Second Reader

Chairman, Command, Control and
Communications Academic Group

Academic Dean

ABSTRACT

The Joint Deployment System (JDS) forms the junction among deliberate planning, time-sensitive planning, and the deployment of forces. The WWMCCS Intercomputer Network (WIN) supplies the necessary interconnectivity among the joint deployment community computer systems. In January 1982, the WWMCCS Information System (WIS) modernization program was launched with objectives including the modernization of WWMCCS hardware and software and the transfer from the present WWMCCS network system to the Defense Data Network (DDN). Because of proven WIN unreliability, the JDS required site-unique software development to supplement present WIN software.

Individualized application software, integrated with the improved network reliability and survivability of the DDN, will enhance the present C3 system. This thesis demonstrates that the total implementation of the WIS involves additional modifications in site-unique applications, standardized procedures for software development, updated hardware technology, and a multi-level security system.

TABLE OF CONTENTS

I. INTRODUCTION 8
- A. PURPOSE 8
- B. MILITARY C3 NETWORK 9
- C. WWMCCS 10

II. WWMCCS INFORMATION SYSTEM 15
- A. BACKGROUND 15
- B. SYSTEM DESIGN 16
- C. SYSTEM STRUCTURE GUIDELINES 18
- D. IMPLEMENTATION 19
- E. EVALUATION/COMPARISON EFFORT 20
- F. DEFENSE DATA NETWORK 23
- G. WIS/DDN CONNECTION 31

III. JOINT DEPLOYMENT SYSTEM 34
- A. BACKGROUND 34
- B. JDS/WIN LINK 35
- C. ADP GOALS AND CAPABILITIES 37
- D. DEVELOPMENT 39
- E. FUNCTIONS 40
- F. REMOTE USER'S PACKAGE 43

IV. WWMCCS/JDS PERFORMANCE 45
- A. SOFTWARE 46
- B. HARDWARE 48
- C. IVY LEAGUE 82 49
- D. COMMUNICATIONS PROCESSOR LOADING 50
- E. NETWORK FRAGMENTATION 53
- F. RESOURCE CONTENTION 55
- G. JDS RESOURCE CONTENTION 59
- H. MANAGEMENT OF COMPUTER OPERATIONS 60

V. RECOMMENDATIONS AND CONCLUSIONS 63
A. SOFTWARE 63
B. HARDWARE 66
C. COMMUNICATIONS PROCESSOR 67
D. NETWORK FRAGMENTATION 69
E. RESOURCE CONTENTION 70
F. JDS RESOURCE CONTENTION 72
G. CONCLUSIONS 74

LIST OF REFERENCES 76

INITIAL DISTRIBUTION LIST 79

LIST OF FIGURES

2.1	User Support Overview	17
2.2	WIS Architectural Segments	21
2.3	DDN/Replica Annual Costs	24
2.4	DDN Transition Plan	33
3.1	WWMCCS/Joint Deployment Community Relationship	36
3.2	Overview of Military Planning and Deployment	42
4.1	JDA Configuration	52

I. INTRODUCTION

A. PURPOSE

In the late seventies time-frame, the Joint Deployment Agency (JDA) experienced unsatisfactory WWMCCS Intercomputer Network (WIN) reliability for large data transfers to remote sites. The WWMCCS Information System (WIS) modernization program addresses the WIN deficiency issues of power supplies and multi-level security and proposes changes in the WWMCCS network to allow greater interconnectivity among sites.

This thesis attempts to assess the WIS modernization impact on large software systems in the WWMCCS community, in particular, the Joint Deployment System (JDS). Specific deficiencies in areas of hardware and software, survivability, and management will be addressed and planned improvements analyzed. The modernization program should improve computer interconnectivity among the joint deployment community in the future, but the command-unique software and WWMCCS standard software modifications will provide the operational reliability necessary for operations in the interim. With the conglomeration of subnetworks into the Defense Data Network during the 1983-1986 time-frame, plus the future WIS support of these command-unique software applications and the improved WWMCCS Network, the joint deployment community may experience a more reliable system for computer resource sharing.

B. MILITARY C3 NETWORK

The Worldwide Military Command and Control System (WWMCCS) of the United States centers around the needs of the National Command Authority (NCA). A Command, Control and Communications (C3) process can be considered an uncertainty reducing technique which aids the commander in the control of forces. A good C3 system must permit the secure and timely flow of information to points both inside and outside the Department of Defense (DOD). This flow must exist during all scenarios -- day-to-day activities, crises, conventional conflict, and nuclear war. The C3 system is a major ingredient to the U.S. national goal of deterrence of war. [Ref. 1: p. 53]

Using WWMCCS, the NCA communicates its desires for deployment of military forces to the Joint Chiefs of Staff (JCS). In short, the JCS mission can be defined as the execution of national decisions. This mission is supported by various communications networks and command and control systems, one of the most central being the Joint Deployment System (JDS) which provides a bridge between the deliberate planning process and time-sensitive planning and execution. Connectivity for these systems is provided by the National Military Command System (NMCS) which consists of three command centers: the National Military Command Center (NMCC), the Alternate National Military Command Center (ANMCC), and the National Emergency Airborne Command Post (NEACP). Also included in the NMCS are the various personnel and equipment necessary for adequate control of forces. [Ref. 2: p. 36]

The Defense Communications System (DCS) is the foundation for worldwide communications during both peacetime and crisis situations. The DCS covers the United States, Europe, and the Pacific area with networks such as the

Automated Voice Network (AUTOVON), the Automated Secure Voice Network(AUTOSEVOCOM), and the Automated Digital Network (AUTODIN). WWMCCS was established in 1962 and supports the command functions of the NCA by supplying information through an online data base system. Although communications is a fundamental aspect of a C3 system, simply having good communications does not equate to an adequate command, control, and communications system. The proper balance of command and control and communications, in union with forces, results in maximum force effectiveness. [Ref. 3: p. 40]

C. WWMCCS

WWMCCS evolved in the early 1960's from a loosely knit conglomeration of about 158 computer systems, using 30 different software systems, and operating at 81 locations; all serving the JCS, Unified and Specified commands, and the Service commands. The majority of these systems were developed independently, consequently the lack of interoperability within the total system proved detrimental to its meeting the NCA requirements for intercommunications among sites. As the concepts of C3 grew, additional requirements were demanded of the system; these requirements were met sporadically, and by 1970, there was an evident need for a WWMCCS modernization effort. In June of 1970, the WWMCCS Automated Data Processing (ADP) Program was initiated to improve WWMCCS support. The program's goals included:

(1) reduction of cost through standardized hardware and software

(2) development of a viable Data Base Management System (DBMS) for data retrieval

(3) standardization of data formats

(4) centralization of management activities [Ref. 4: p. 2]

Prior to this effort, the WWMCCS program had no central authority for its budgeting or management. Numerous organizations were responsible for the various aspects of the program; for instance, the WWMCCS Council provided policy guidance for development and operation of the system; the JCS evaluated WWMCCS' overall effectiveness; various Assistant Secretaries of Defense provided advice on system design and development, warning and intelligence matters, and ADP procurements; and each service was responsible for funding its equipment acquisition and software development. The WWMCCS System Engineering Office (WSEO), a separate organization in the Defense Communications Agency (DCA), was organized in the mid 1970's to coordinate the general system engineering of WWMCCS. One of the biggest disadvantages to the WWMCCS management structure was that the Director, DCA, also Director, WWMCCS Engineering, reported to two organizations: the Assistant Secretary of Defense (C3I) for organization and technical matters and the chairman of the JCS for doctrine, operational policies, and validation of requirements. This, compounded with the fact that the Director, DCA, had no authority for the budgeting or management of the WWMCCS program, precluded the successful coordination of WWMCCS ADP development efforts. [Ref. 5: p. 8]

The WWMCCS ADP Program also outlined a set of well-defined requirements which included the capability to process large amounts of data within a reasonable time, reliability greater than 99%, user and maintenance friendliness, and small physical space and personnel requirements. [Ref. 6: p. 22]

The WWMCCS functions which support related missions are grouped to allow each family of functions to be independently defined and implemented. Interfaces among the functional families are well defined. One of the basics of the WWMCCS architecture is the concept of four distinct functional families which support the NCA, JCS, and Unified and Specified Commands. They are:

(1) Resource and Unit Monitoring (RUM)

(2) Conventional Planning and Execution (CPE)

(3) Nuclear Planning and Execution (NPE)

(4) Tactical Warning/Attack Assessment and Space Defense (TW/AA and SD) [Ref. 7: p. 1-1]

In addition, WWMCCS ADP is divided into three categories. Category A includes the WWMCCS standard software, the backbone of WWMCCS ADP which principally supports the command and control requirements. Category B is that software which is unique to a particular activity. And Category C encompasses the newly emerging systems. [Ref. 8: p. 2]

As WWMCCS grew, utilization of the WWMCCS Intercomputer Network (WIN) increased. The network was initiated as a prototype at three sites and from 1977 to 1983 the number of WIN sites jumped from six to twenty-three, with future plans eventually including all WWMCCS sites. Commonly used functions include:

(1) maintenance of status and location of forces and resources

(2) planning for force mobilization and deployments

(3) preparation of the Single Integrated Operations Plan (SIOP)

(4) estimating and monitoring Navy fleet fuel consumption

(5) assisting in preparation and processing of AUTODIN messages [Ref. 9: p. 5]

The utilization of the Joint Deployment System (JDS) contributed to the increased activity on the WWMCCS network. As a primary function, the JDS maintains Time-Phased Force Deployment Data (TPFDD) files for specific Operation Plans (OPLANs) outlining the supported commander's concept of operations and requirements. [Ref. 10: p. 11] Prior to additional software development, these files were sent to WIN subscribers in their entirety to initiate JCS exercises. As the TPFDD files were updated throughout the exercise, the entire file was again sent to all users. These large data transfers, coupled with an overall increase in WIN usage, placed a burden on network components and host processors, causing WIN performance to reach an unsatisfactory level. Particular site-unique development included the JDS Remote User's Package (RUP), discussed in Chapter 3.

A new surfacing problem was the lack of a Multi-Level Security (MLS) system. A MLS system allows users with varying security clearances to simultaneously share computer equipment with access to various software allowed on a case-by-case security check. One theory for implementing a MLS system is the usage of rings of protective organization for the hardware. Here, the operating system is segmented into N-rings, with N greater than two. The inner-most ring will be occupied by the core, or kernel, of the operating system. The system software and security processes will be run here; for instance, validation of passwords and data access requests. The resource allocation software should reside in a seperate ring for scheduling of tasks and computer resources. The outer rings are available to the users for processing application programs. Routines in Ring 'i' have access to Rings 'i' and all rings greater but can only access more inner rings through procedure calls, thus affording the proper security check opportunity. The rings of protection secure sensitive software and data and also act as firewalls against user damage. [Ref. 11: p. 540]

It is interesting to note that in the mid-1960's the Massachuset's Institute of Technology, Bell Telephone Laboratories, and the computer department of the General Electric (GE) Company developed one of the first operating systems to employ rings of protection, the Multiplexed Information and Computing System (MULTICS). The original MULTICS was installed on a GE645, later a Honeywell Information System (HIS) 645 computer, and in 1973, replaced by the HIS 6180. The HIS 6180 supports eight rings of protection: the operating system uses Rings 0-3; Rings 4-7 are available to the users. [Ref. 11: p. 535] With no MLS system, all machines, terminals, and personnel on the WIN must be cleared to the highest level being utilized. [Ref. 12: p. 7]

Other problems included the lack of a long-range plan for WWMCCS/WIN development and the early 1960 Honeywell architecture which is not the state-of-the-art for an online query and response system.

A misconception was also prevalent concerning WWMCCS -- that it would provide communications between the President and the foxhole. This was never the design intention of WWMCCS; however, what was desired was a communications network for several command echelons and a reliable military command and control system connecting the NCA to the executing commanders. [Ref. 1: p. 40]

Although the reliability of the WWMCCS Intercomputer Network (WIN) had fallen below a satisfactory level, the WWMCCS ADP sites utilized the on-site Honeywell computer equipment to develop software applications for unique requirements. By the mid 1970's, there was a great dependency on WWMCCS ADP for day-to-day operations and crisis/exercise support and the need for a reliable computer network became obvious. [Ref. 12: p. 7]

II. WWMCCS INFORMATION SYSTEM

A. BACKGROUND

In November 1981, the Deputy Secretary of Defense decided the WWMCCS Information System (WIS) modernization plan needed a focal point for coordination to receive policy and guidance directives from the JCS. In January 1982, a WIS Joint Program Manager (JPM) was appointed to control the joint modernization activities of WWMCCS ADP and the development of all telecommunications interfaces. Small site-unique enhancements will continue to be processed normally. The WIS JPM receives direction from the JCS and reports through the JCS to the Secretary of Defense. [Ref. 8: p. 44]

A System Progam Office (SPO) was established within the Air Force Electronic Systems Division to manage WIS acquisition and provide support in such areas as architecture and system engineering. The SPO also maintains Air Force programming and budgeting data for the WIS modernization plan. [Ref. 8: p. 44] The Director, DCA and the WIS JPM have signed a Memorandum of Agreement which specifies the guidelines for the Command and Control Technical Center (CCTC) support to the WIS modernization effort.

The basic goal for the WIS modernization program is to provide the NCA, JCS, and Unified and Specified commanders with real time access to status and warning information. WIS objectives include: improved WWMCCS performance, greater WIN reliability, modernization of WWMCCS ADP harware and software, and increased ADP security. Of the three WWMCCS ADP categories mentioned previously, WIS will centralize its effort on Category A -- WWMCCS standard

software. Of the four functional families of operational requirements, WIS will focus only on two: Resource and Unit Monitoring (RUM) and Conventional Planning and Execution (CPE). The Air Force will continue to manage the WWMCCS ADP systems in the Nuclear Planning and Execution (NPE) and Tactical Warning/Attack Assessment and Space Defense (TW/AA and SD) areas. [Ref. 8: p. 18]

E. SYSTEM DESIGN

The WWMCCS Information System (WIS) was designed as an interactive network system in which a user at any command or agency can communicate with a user/host at any other command or agency also connected to the network. The Defense Data Network (DDN) will provide the interconnection among WWMCCS sites. A Network Operations Center will monitor the network as a separate node on the DDN. Local area networks (LANs) will exist for secure and interactive communications. The advantages to LANs include: usual ease in configuring systems to meet specific site requirements, development of standard components for common functions, flexibility for selective modernization, and the ability to develop incremental security solutions. Figure 2.1 graphically depicts the user support scheme envisioned by WIS.
[Ref. 8: p. 3]

The WIS system objectives include:

(1) user-friendly interface development

(2) data processing capabilities for all WWMCCS sites

(3) reliable inter-command communications

(4) improved processing capabilities during battle conditions [Ref. 8: p. 15]

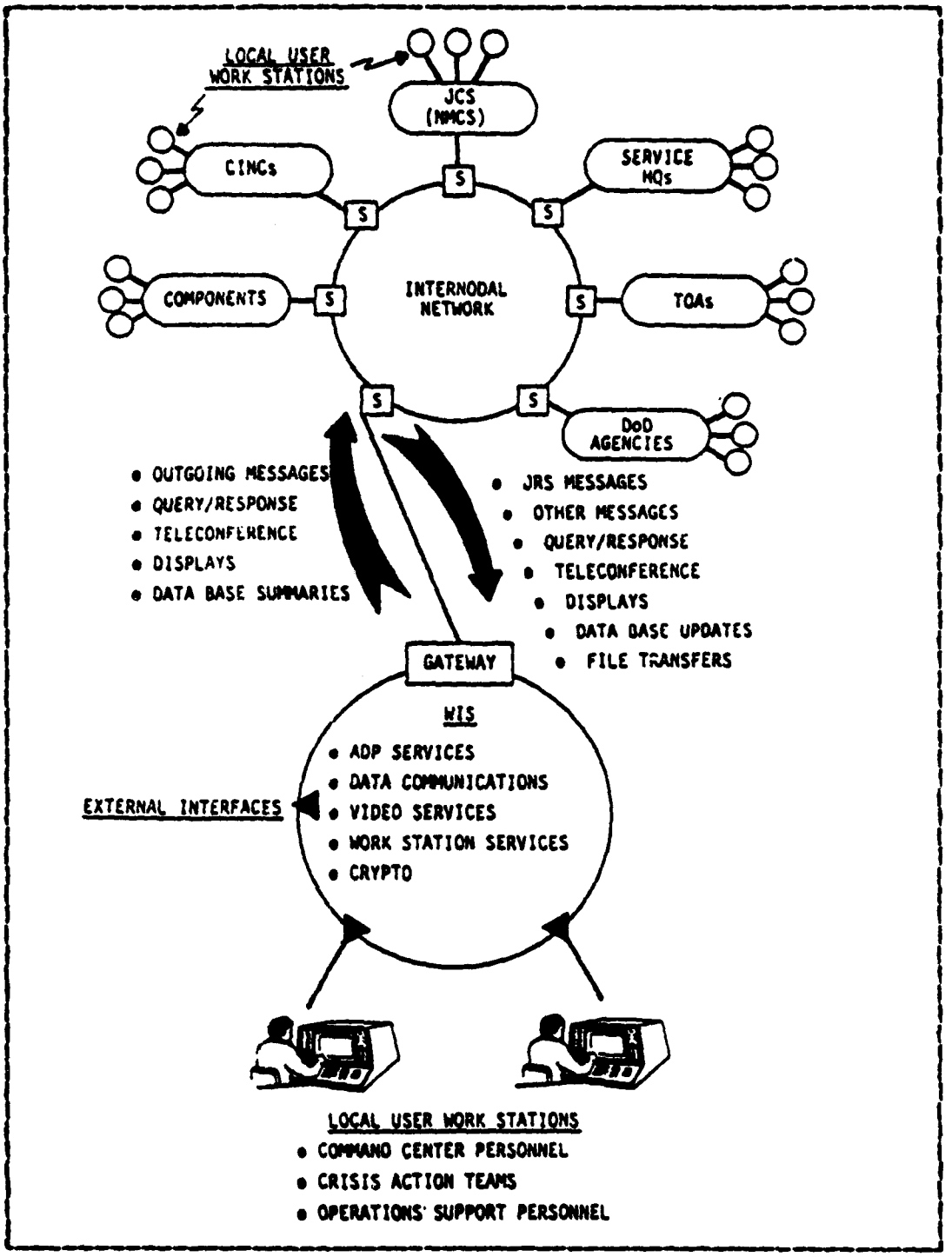


Figure 2.1 User Support Overview.

Projected WIS characteristics to accomplish these goals are divided into three categories: access, availability, and modularity.

Access characteristics:

(1) organic WIS support for major sites
(2) remote access capability for small sites
(3) user access from a single work station
(4) a multi-level security system
(5) minimum site training requirement

Availability characteristics:

(1) secure and interactive network
(2) operational for day-to-day and crisis support

Modularity and flexibilty characteristics:

(1) accomodation of a wide range of sites
(2) standard software
(3) minimum implementation disruption
(4) state-of-the-art technologies considered

[Ref. 8: p. 16]

C. SYSTEM STRUCTURE GUIDELINES

The WIS JPM Office has developed guidelines for WIS system requirements in the areas of standardization, security, and system characteristics.

Hardware standardization will not be mandatory because of the numerous existing systems and the competitive procurement possibilities. Software development standardization will be achieved through the exclusive use of ADA as the program design language. Standard, pre-determined protocols will set the intercomputer communications standards. Routine and emergency maintanance will be monitored by a single organization; maintenance standards will be imposed. To facilitate cooperation among the remote sites, data definition standards will be implemented. [Ref. 8: p. 31]

The core of the WIS security program lies in the multi-level secure LANs with secure interfaces to all other WIS components. Authentication for users will be applied as a security control with an audit capability available. DCD security requirements require that a multi-level security system be achieved within the WIS modernization program. [Ref. 8: p. 34]

The WIS modernization program will provide capabilities to improve communication survivability and ADP support to WWMCCS sites. Some proposed capabilities are:

(1) distributed and/or redundant processing with remote access
(2) graceful degradation
(3) rapid restart and recovery
(4) distributed data files
(5) transportable systems

Standards for accessibility include the ability to access all WIS-related capabilities from a single workstation. Other required system capabilities are flexibility, reliability, maintainability, and interoperability. [Ref. 8: p. 35]

D. IMPLEMENTATION

WIS will be implemented during four modernization segments and utilizing four major contracts. The Maintenance Segment includes the near-term enhancements to the baseline hardware and software to stabilize WIS performance and will be accomplished through the Integration Contract. Next, the Transition Segment, linked to the Common User contract, transfers the user communities from the existing WWMCCS ADP to the WIS modular architecture for future modernization and initiates the Automated Message Handling capabilty. The Joint Mission Segment concentrates

on the common applications software modernization; the Joint Mission Hardware contract will provide the standard hardware base and supporting operating system by late FY85. The final segment will be the Service and Command unique application software improvements which will be the responsibility of the Services and user commands. Figure 2.2 illustrates the WIS growth through the four modernization segments. [Ref. 8: p. 3] The last major contract, the Configuration Management contract, provides for independent validation of the software provided by the Integration and Common User contractors. In addition, this contractor will assist the WIS JPM in the overall configuration management of WIS. [Ref. 13: p. 9]

E. EVALUATION/COMPARISON EFFORT

As mentioned earlier, one of the major problems in the WWMCCS community is the unsatisfactory performance of the WWMCCS Intercomputer Network (WIN). In September 1981, Director, DCA organized an effort to investigate the replacement of the present WWMCCS network system with a more contemporary system.

Initially, the idea surfaced to take advantage of the proven AUTODIN I technology and develop an AUTODIN II. It was envisioned that AUTODIN II would provide a common user data network with a multi-level security system to meet network requirements through 1985. In 1976, the contract was awarded to Western Union, Inc. and the Initial Operational Capability (IOC) was set for January 1979. [Ref. 14: p. 44]

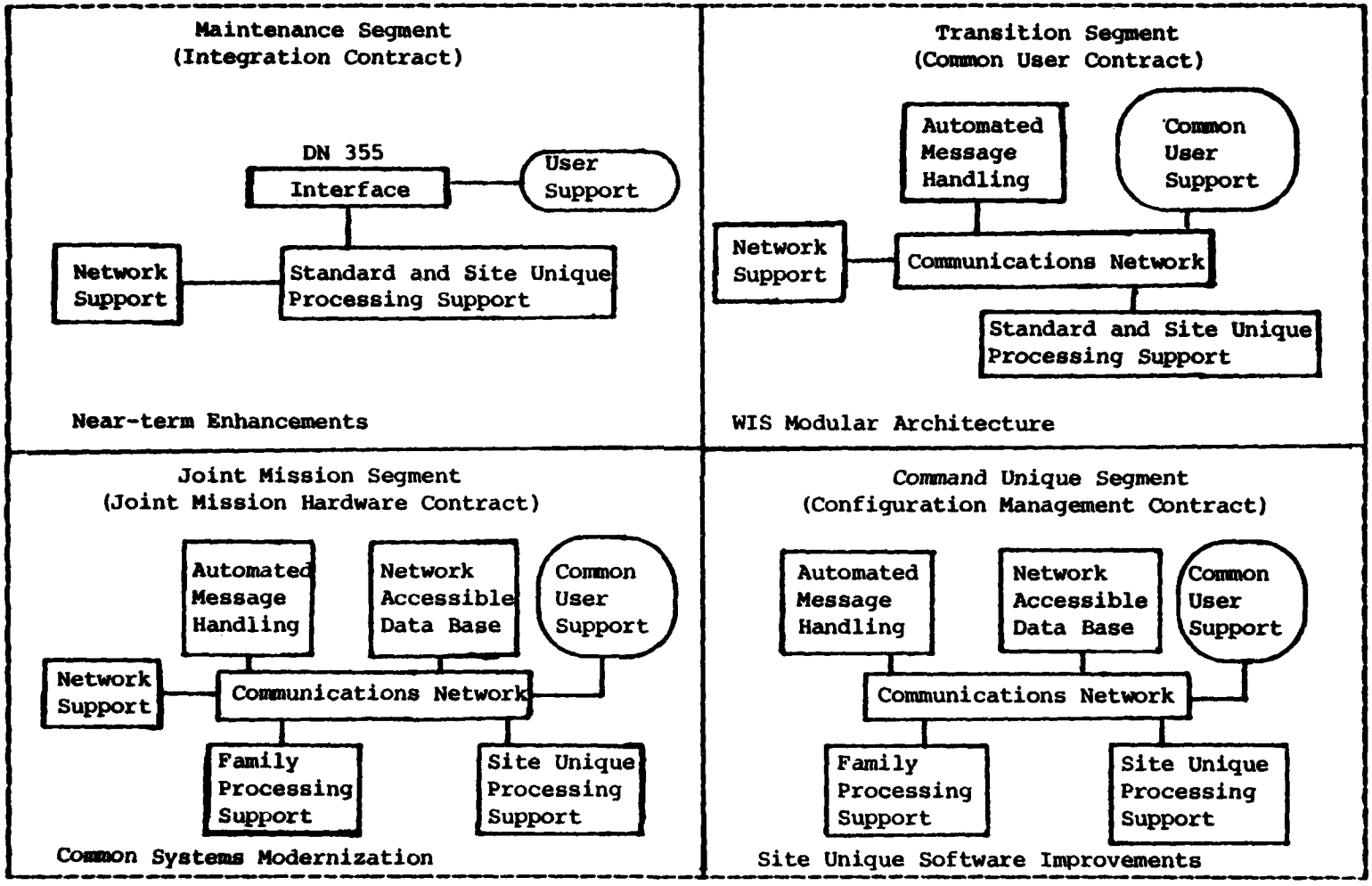


Figure 2.2 WIS Architectural Segments.

Beginning in 1979, the IOC date was extended several times until July 1980, when the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASDC3I) requested a review of the AUTODIN II project with some possible alternative proposals. In July 1981, the Deputy Under Secretary of Defense for C3I (DUSDC3I) questioned the wartime survivability of AUTODIN II. The doubt focused on one of the basic design criteria for the system -- a small number of switching nodes. These switching nodes would require manning and would be relatively expensive. Immediately after this, the Air Force Test Director issued a report concerning the increasing cost of the system and doubts about the technology and future system performance. [Ref. 14: p. 45]

In late 1981 the Director, Defense Communications Agency (DCA) established three design teams:

Team 1 -- tasked with designing the best possible, survivable AUTODIN II system

Team 2 -- tasked with designing the best alternative which would be based on the ARPANET and WIN technology, a Replica approach

Team 3 -- a 30-day evaluation team.

The evaluation team was to establish guidance for the two design teams and develop evaluation criteria. [Ref. 14: p. 45] Some of the evaluation factors considered were survivability, security, system design, and cost. The ARPANET replica proposal, referred to as the Replica, seemed better able to withstand network element losses, proposed a more flexible routing algorithm, and afforded a greater mobility capability. [Ref. 15]

AUTODIN II now had a six-year old design and, because of continuous technology advances, the expected life of a computer system is about eight years. In the area of large data transfers, AUTODIN II was superior to the Replica

design. The Replica design would be using smaller packets for message transfers throughout the network -- smaller packets necessitate more numerous packets which in turn increase the overhead traffic through the system and can degrade system performance. If AUTODIN II had been available for implementation during the evaluation effort time frame, the technology, schedule, and cost risks associated with the Replica proposal would certainly have cancelled some of the benefits. However, having no satisfactory AUTODIN II system online, the benefits of the Replica approach justified the risks. [Ref. 15]

In constant FY82 dollars, AUTODIN II total system cost was estimated at $588 million where the Replica total system cost was $429 million. It was projected that the AUTODIN II annual operating costs would steadily increase to $72 million until 1995, where the annual cost would level off near $55 million. The Replica system annual cost is expected to peak at $71 million around 1985 and steadily decrease to the $40 million range in 1987. Figure 2.3 shows DDN/Replica annual costs. [Ref. 15]

In February 1982, the evaluation was completed. Based on the conclusions the Director of DCA decided the Replica approach would provide a better DOD data network. Consequently, the Deputy Under Secretary of Defense ordered the termination of the AUTODIN II network and the initialization of the Replica design, to be known as the Defense Data Network (DDN). [Ref. 14: p. 45]

F. DEFENSE DATA NETWORK

The Defense Data Network (DDN) will provide the WIS community with the secure, reliable, interactive network necessary to perform its functions. The DDN is designed as a single, integrated packet-switching data network. The

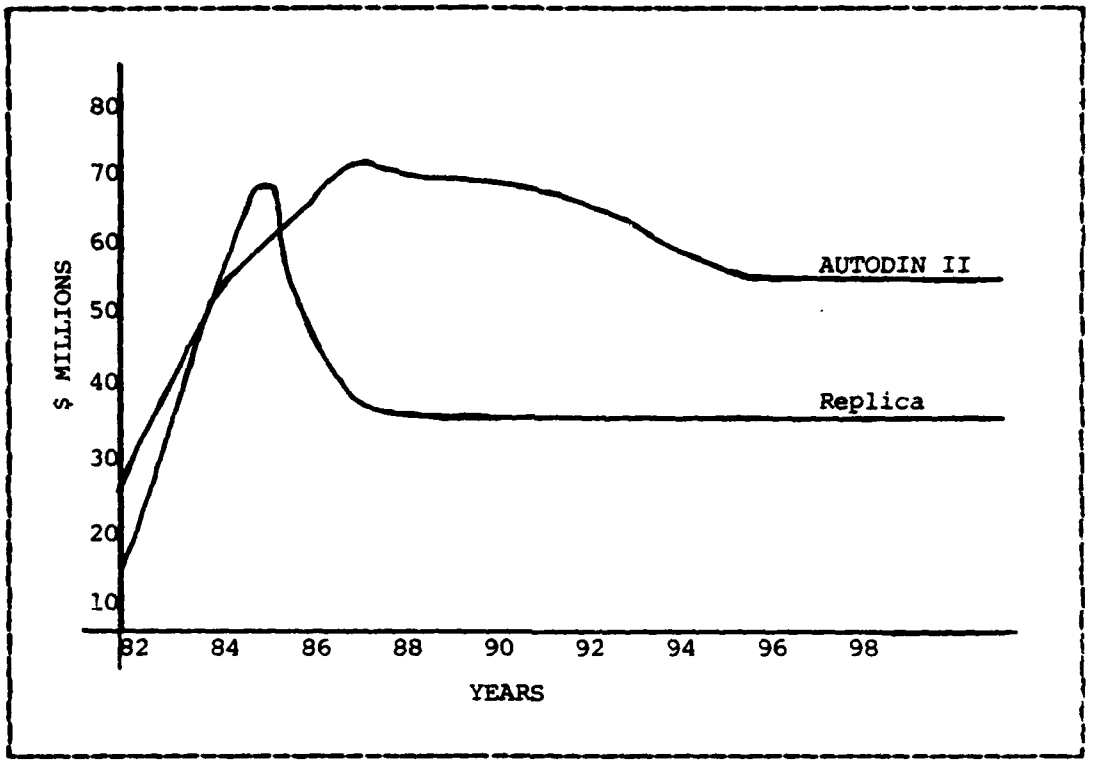


Figure 2.3 DDN/Replica Annual Costs.

completed network will have 91 subscriber systems with approximately 488 hosts and 1,446 terminals. There will be 171 switching nodes at 85 sites. The DDN meets the Worldwide Digital System Architecture (WWDSA) standards and objectives by providing a solid technology base, low risk, and a cost effective system. This network will satisfy current survivability requirements during a crisis and meet DOD intercomputer telecommunication requirements supplied by the JCS. [Ref. 16: p. 2]

The major DDN design concepts are standardized components, distributed switching nodes, and automatic fault recognition. Standardized components allow smaller development costs and lower maintenance and support costs. Also,

component modularity reduces the maintenance impact. Distributed switching nodes aid in eliminating choke points which increases the overall survivability of the system. A wide distribution of switching nodes usually minimizes any impact after a single node failure. Another major concept, the DDN automatic fault recognition system, is implemented through a series of Monitoring Centers (MCs) which are in continuous operation to monitor network performance and identify trouble areas.

The network Monitoring Centers will be key nodes on the DDN network. There will be a principal system MC, an alternate MC, regional MCs for Europe and the Pacific area, and a MC for each keyed community. Primary functions for the monitoring centers will include:

(1) monitoring the status of the network

(2) isolating network faults

(3) supporting software maintenance

(4) providing network element information [Ref. 16: p. 5]

The Defense Data Network will provide four levels of support to the current WWMCCS community:

Level 1 -- host processor sites for Resource and Unit Monitoring (RUM) and Conventional Planning and Execution (CPE) support

Level 2 -- limited on-site processor support plus access to remote host processors

Level 3 -- processor support through network access to remote processors in Hawaii

Level 4 -- support through individual terminals connected to remote host data processors [Ref. 8: p. 27]

The Defense Data Network is designed for continuous operation to support real time handling of all user's traffic. The availability goal is greater than 99% for any

pair of users. [Ref. 17: p. 5] The three major DDN system elements are switching nodes, IPLIs, and Mini-TACs.

The switching node used for the DDN is a Bolt Beranek and Newman (BBN) C/30 switch, a microprogrammed minicomputer designed for unattended operations which eliminates the need for DDN dedicated personnel at each switching node. The throughput capability of each C/30 node is 300 packets per second in tandem processing -- 300 packets in, 300 packets switched, and 300 packets out simultaneously, for a total of 900 packets being handled. The long term reliability goal is 5000 hours or greater for Mean Time Between Failures (MTBF). The development risks are low since the C/30 switch and its software are functioning elements on such networks as the ARPANET; WIN; Community On-Line Intelligence Network (COINS); Intelligence Data Handling System, Communications (IDHSC); and the European Movement Information Network (MINET). Technology risks are considered low since only minor modifications are neccessary. [Ref. 16: p. 33]

The Internet Private Line Interface (IPLI) is based on the Private Line Interface (PLI) which has been used on the ARPANET and other networks for more than five years. The PLI/IPLI technology allows the simplest of end-to-end encryption available. An ILPI will reside between a host and switching node or Mini-Terminal Access Controller (mini-TAC) and switching node, depending on site configuration. The IPLI is currently under development with an initial delivery date of July 1983. It will support the standard DOD protocol, Internet Protocol (IP), and widespread deployment is expected because of reduced cost, size, and power and weight requirements from the PLI currently being used. The IPLI hardware consists of a KG-84 cryptographic device and two Motorola MC68000-based packet processors. A minimum of fifty packets per second is set as a throughput goal and the MTBF goal is at least 5000 hours.

The Mean Time To Repair (MTTR) is expected to be approximately thirty minutes with an availability of 99.9%. The IPLI requires no additional personnel and the maintenance and monitoring systems may be operated from a remote site. The development risk involved is considered low due to the traditional architecture used. [Ref. 14: p. 39]

A Mini-Terminal Access Controllor (mini-TAC) is a terminal access device which allows a cluster of up to sixteen terminals simultaneous access to the network. The hardware of a mini-TAC is a MC68000 microprocessor with memory and multiple network interface ports. The mini-TAC software is based on the software developed for use on the ARPANET and allows terminal users to establish connections between their terminals and an arbitrary host on the network. The DOD standard IP and Transmission Control Protocol (TCP) are used. The MTBF goal is greater than 5000 hours and the board-swapping capability simplifies maintenance. Since the mini-TAC is also designed for unattended operations, no dedicated personnel are required. Control monitoring and hardware/software fault isolation can be accomplished remotely by the MCs. Mini-TAC availability is expected during FY84. [Ref. 16: p. 42]

One of the major comparison factors for the AUTODIN II/DDN evaluation was survivability. The small number of nodes proposed for the AUTODIN II system left major doubt as to its survivability. DDN's survivability features include:

(1) redundancy -- the final system will comprise 171 switching nodes, 9 fixed monitoring centers, and 5 mobile reconstitution nodes with MC capability

(2) disseminated switching nodes -- geographically dispersed sites afford the higher priority users a greater chance of reconstitution

(3) a dynamically adaptive routing algorithm which automatically reroutes traffic around heavily congested or damaged links and nodes

(4) graceful degradation because of the network's response to damaged nodes

(5) four levels of precedence/preemption processing

(6) hardening and HEMP protection including electromagnetic shielding, line isolation, and power surge protection

(7) reconstitution -- the five mobile reconstitution nodes will be positioned in areas less likely to be targeted and all users will have a detailed alternative routing plan

(8) preplanned rehoming -- all users will have a priority listing of switching nodes for rehoming [Ref. 16: p. 125]

DDN security will be accomplished through link encryption, end-to-end encryption, and physical and procedural security measures. The KG-84 cryptographic devices will provide the necessary link encryption. The Internet Private Line Interface (IPLI) devices between the host and switching node or mini-TAC and switching node will provide the end-to-end encryption. The IPLI will also separate subscribers operating at different system security levels. For physical security measures, all switching nodes will be TEMPEST enclosed and located in secure military facilities. Only System Monitoring Center (SMC) personnel will be able to retrieve traffic statistics. All personnel at regional and system MCs and personnel with access to switching nodes will hold a SECRET clearance. In addition, personnel with access to a MC for a secure subnetwork must also be cleared to the highest security level of the subnetwork subscribers. [Ref. 16: p. 12]

The DDN program office is within the DCA organization and consequently comes under DCA's staffing and policies. The National Security Agency (NSA) has the responsibility for certifying and accrediting the IPLI devices and

analyzing the network system design for use with classified traffic. DDN subscribers will be responsible for acquiring the necessary hardware and software for DDN operation and support. [Ref. 14: p. 258]

Another major factor considered during the evaluation phase was cost. According to the evaluation team, the "DCN I system can provide DOD with a survivable, common-user system at a cost less than being paid for the dedicated systems...". [Ref. 16: p. 15] Using FY82 dollars, the 91 dedicated systems listed in the user requirement data base cost over $35.2 million for annual operation. The annual cost for the new DDN system includes:

System Management	3,354 K	(10.3%)
Trunk/Access Lines	24,694 K	(7.6%)
Operations and Management	4,428 K	(13.6%)
Total	$32,476 K	Annually

When development and acquisition costs are included, DDN annual operating costs average $35.549 million over a ten year period. [Ref. 16: p. 255]

The Defense Data Network system design builds on three operational networks which use the BBN C/30 switching node and accompanying software:

(1) ARPANET -- with 90 nodes at 75 locations

(2) WIN -- with 26 nodes at 16 locations

(3) MINET -- with European locations [Ref. 17: p. 2]

The DDN will employ a four stage implementation approach which should lead to a graceful evolution capitalizing on existing networks and interfaces with minimum risk for new technologies. The ARPANET will supplement DDN's test and development facilities but will remain as a scaled-down research network. It will later serve as an operational testbed for future DDN software releases. [Ref. 16: p. 24]

The four transition stages for DDN I are:

Stage 1 -- Service will be provided to subscribers that can be handled with minimum development. The WWMCCS Network C/30 switch upgrade will be accomplished during this stage. Communities of interest and networks with differing security levels will be physically separated into three distinct networks:

(1) Strategic Air Command Digital Network (SACDIN) -- at a Top Secret (TS) system-high security level

(2) Military Network (MILNET) -- for unclassified subscribers to include military ARPANET users

(3) Command and Control Intelligence (C2I) Network -- with a TS system-high security level network with two subnetwork communities:

the C2 Community basically for WIN subscribers and the Intelligence Community primarily for IDHS II/Department of Defense Intelligence Information Systems (DODIIS) users.

Stage 1 is expected to be completed by end of FY83.

Stage 2 -- As additional IPLIs become available during 1984, more subscribers will be added to the network. The mini-TACs will be implemented in Stage 2, also. Completion is expected by the end of FY84.

Stage 3 -- During Stage 3, the three separate networks originated during Stage 1 will be integrated to become the DDN I, supporting multiple levels of security. During this stage, additional classified subscribers will be incorporated into the network. Stage 3 will be completed by the end of FY85.

Stage 4 -- As host interfaces are developed, all remaining DDN subscribers will be included in the network. The final DDN I network will consist of 171 nodes supporting 91 systems, and the DDN system design allows for a moderate increase in traffic from each network user. [Ref. 16: p.

189] Figure 2.4 shows the transition plan for the DDN I. [Ref. 16: p. 190]

G. WIS/DDN CONNECTION

Currently, the Defense Communications Agency provides WWMCCS software support through the Command and Control Technical Center (CCTC). Although the WIS modernization plan is not a part of DCA, the WIS JPM and the Director of DCA have entered a Memorandum of Agreement which insures CCTC support during the WIS modernization effort. However, since plans call for the Defense Data Network (DDN) to be integrated into the DCS, the DDN program office falls under the DCA organization. The DDN will provide a common user network, capable of incorporating the majority of the C3 networks available today and providing a standard, secure and shared-resource capability.

The DDN will not be restricted to support of the WWMCCS community. As can be seen from Figure 2.4, networks such as the SAC Digital Network (SACDIN) and the ARPANET will utilize the Defense Data Network for intercommunications among member sites. With these various user communities riding on one network system, a multi-level security system is imperative, although technology hinders the development of such a system. The management of the DDN network, a network where users range from unclassified military users on the ARPANET to high classification users of the JDS on the WIN, has not been sufficiently addressed and will become the source of major problems.

As DDN comes into being, new WWMCCS standard software will be implemented under the WIS modernization plan and existing site-unique software will be modified to reflect the updated system. These software changes and future hardware acquisitions will affect every system used within the

WWMCCS community. The WIS modernization impact will be felt by all users supported by the Joint Deployment System (JDS), one of the most widely used WWMCCS systems and the total management system coordinating the links between deliberate planning, time-sensitive planning, and deployment of forces.

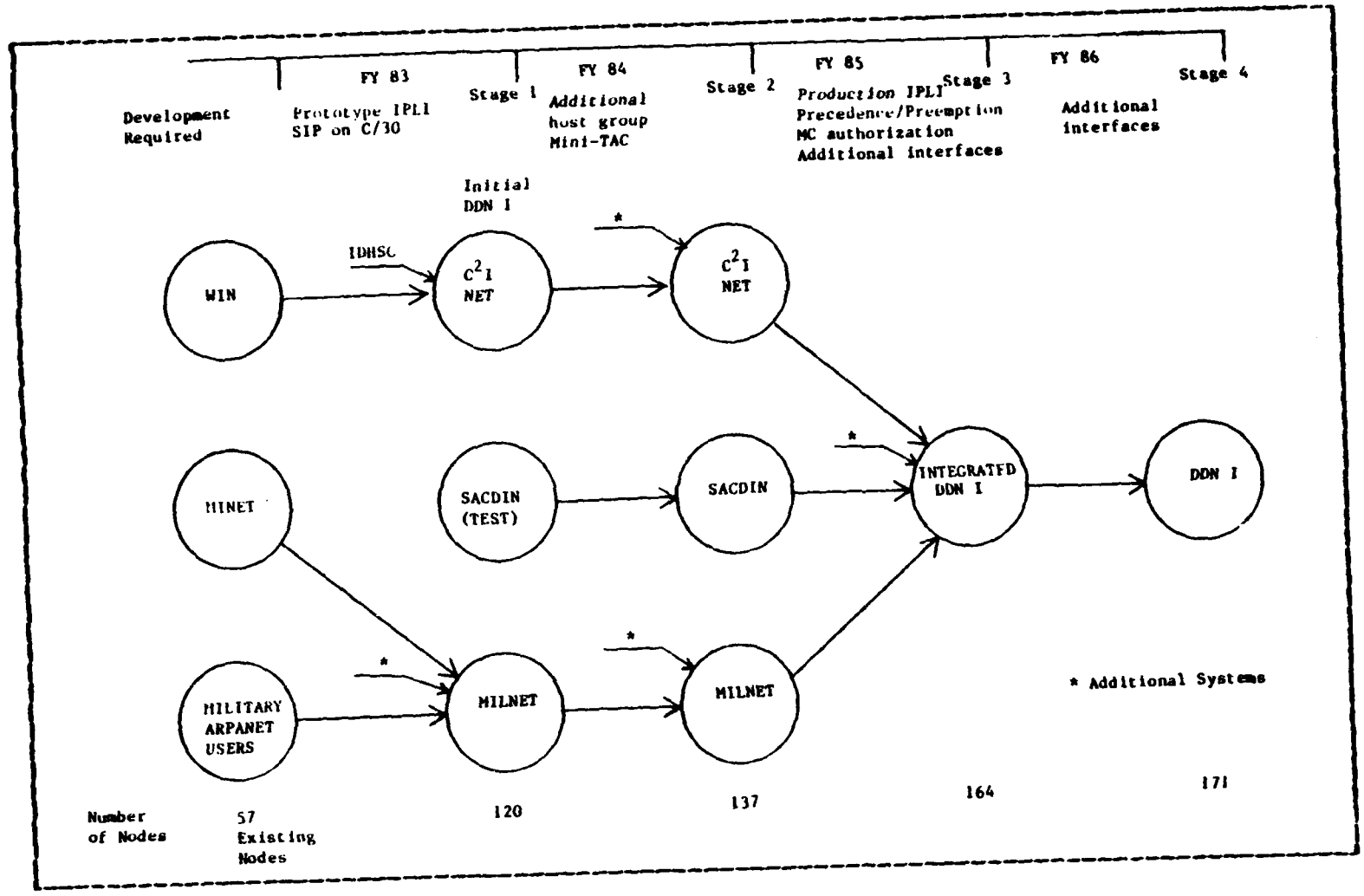


Figure 2.4 DDN Transition Plan.

III. JOINT DEPLOYMENT SYSTEM

A. BACKGROUND

In October 1978, the JCS conducted a command post exercise, NIFTY NUGGET, to test full mobilization and deployment capabilities for U.S. forces. NIFTY NUGGET exposed deficiencies in both the military deployment planning and execution process as well as the supporting Management Information System (MIS). The systems most widely utilized during NIFTY NUGGET included the Joint Operational Planning System (JOPS), Unit Status and Identification Report (UNITREP) System, and command unique systems such as the Deployment Management System (DEPMAS) used by the U.S. Readiness Command (USREDCOM). JOPS supported planning but supplied no support for the execution phase. The UNITREP system was not responsive to time-sensitive decisions. DEPMAS was not available to the joint deployment community, the system dealt with Army and Air Force forces only. The need for a centralized deployment and decision support system for planning and execution was evident. In March 1979, the Joint Deployment Agency (JDA) was established to support the JCS and supporting commanders as the nucleus of deployment and associated activities. [Ref. 10: p. 3]

The Joint Deployment System (JDS), resident at the Joint Deployment Agency, was created to support the JDA mission. The JDS includes personnel, procedures, directives, communications systems, and electronic data processing systems which support peacetime planning and time sensitive planning and procedures. The JDS concept is the development of a single support system for all stages of deployment management with particular focus on planning, deployment

execution, and crisis monitoring. After the JCS exercise order is delivered, the JDS allows the monitoring of movement of forces, materiel, and non-unit related personnel. The Master Force List (MFL) file, schedule file, scheduling requirements and UNITREP data are generated from the deployment data base and distributed to users. [Ref. 10: p. 18] Through the JDS, the Joint Chiefs can achieve direct implementation of their deployment decisions during peacetime, command post exercises, crises, and war. [Ref. 18: p. 1]

B. JDS/WIN LINK

The mission of the JDA obviously depends on interconnectivity among the joint deployment community. The WWMCCS Intercomputer Network (WIN) is used to organize these geographically separated host computers into a single network and becomes the backbone of the JDS communications system, essential in the planning and execution of deployment decisions. The deployment data base depends on WIN for accurate information exchange between user sites and the JDA. [Ref. 19: p. 1] Figure 3.1 illustrates the WIN relationships within the joint deployment community. [Ref. 20: p. 12]

Transaction throughput is site dependent but a JDA site will usually average 1200 transactions per hour. User response time is dependent on the number of users simultaneously accessing WIN. For example, with an average of ten simultaneous users, WIN response time averages two to five seconds. Ten is considered a small number of users and once over ten, significant performance degradation is experienced. [Ref. 18: p. 13] The WIN software available for transactions include TELNET, the Telecommunications Network

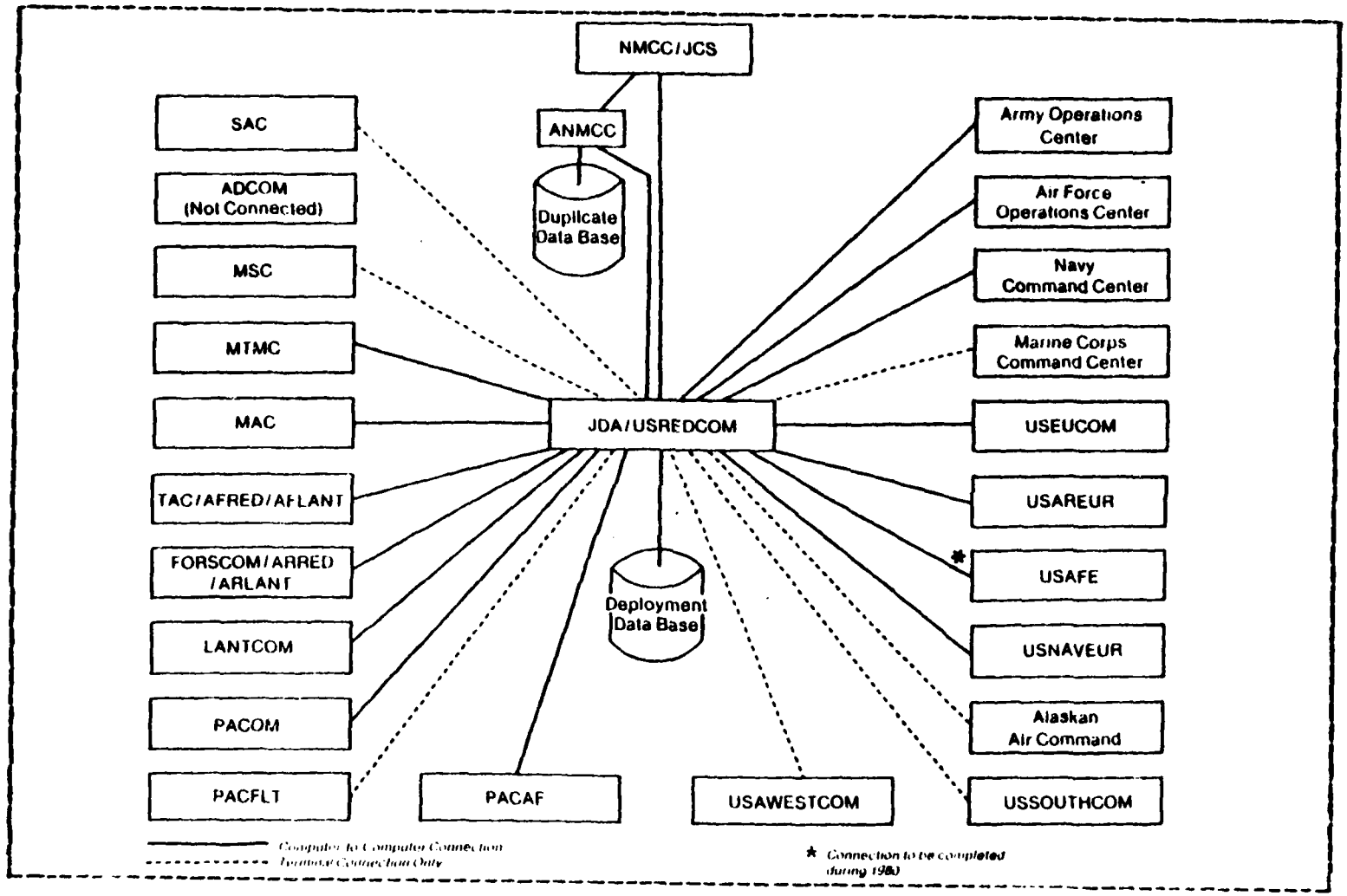


Figure 3.1 WWMCCS/Joint Deployment Community Relationship.

Program used for message exchange and direct access to resources of remote hosts, the File Transfer Service (FTS) used mainly for large bulk transfers between sites (i.e., the TPFDD file and TPFDD file changes), and the Teleconference (TLCF) capability which simultaneously links any number of WIN nodes into a textual exchange conference. AUTODIN is the general message exchange system which may also be used for query/response activities and NACE transfers data between the JDS and AUTODIN, automatically formatting the messages generated by JDS. [Ref. 10: p. 18]

C. ADP GOALS AND CAPABILITIES

The Joint Deployment System ADP criteria goals include an availability of 24 hours a day, 7 days a week, except for scheduled maintenance and unexpected outages. The operation goal is 95% for routine processing and 99% for crisis and exercise operations. The deployment data base is resident at JDA with the major backup at REDCOM. The JDA and REDCOM computer systems are comprised of four processors organized in dual configuration with shared disk drives, colocated in the same facility. The JDS reliability goal for MTBF is 36 hours with MTTR of 10 minutes. When fully developed, JDS will be a transaction-oriented communications system capable of real-time processing on a distributed data base within the WIN environment. [Ref. 10: p. 32]

The JDS computer system availability not only depends on the host computer up/down ratio; other factors include the supporting WWMCCS system software such as the Time-Sharing System (TSS) and the General Comprehensive Operating System (GCOS), the JDS software which includes the Remote User's Package (RUP), and WIN availability. All of these components must be available for a remote user to access the deployment data base. JDS will allow interfaces with

appropriate service and command-unique data systems for accurate information flow among the joint deployment community.

The JDS is divided into 5 procedural subsystems:

(1) plan generation -- expansion of the data base for inclusion of new data

(2) plan maintenance -- modification of the data base to reflect changing resources or constraints

(3) execution preparation -- adjustments to plan data to account for real world dates and requirements

(4) scheduling -- coordination and distribution of transportation schedules developed in conjunction with the Transporting Operating Agencies (TOAs), i.e., Military Airlift Command (MAC), Military Traffic Management Command (MTMC), and Military Sealift Command (MSC)

(5) movement monitoring -- reporting of the status of the deployment, departures, and arrivals [Ref. 10: p. 20]

The Joint Deployment System offers the joint deployment community five processing alternatives:

(1) Time Sharing System (TSS) -- simultaneous access of the computer system by more than one user

(2) batch updating -- primary system for JDS data base control

(3) transaction processing -- data base updating through one of twenty-three Transaction Service Modules (TSMs) which maintain a near real-time information flow between WIN sites

(4) stand-alone programs -- software sent over the WIN network to update the JDS data base

(5) Remote User's Package (RUP) -- provides the capability to send and receive transactions from other WIN sites [Ref. 21: p. 34]

Users may access local or remote deployment data bases using any one of four methods. Twenty-two on-line queries are available on the time sharing system. The Management Data Query System (MDQS) for retrievals allows the user to originate a batch process for information retrieval from the Master Force List (MFL) file and schedule files. The MFL file also allows users without the RUP capability to initiate information queries. Users can also utilize the automatic scheduling messages package to automatically receive movement data for the next twenty-four hours through the NMCC Automated Control Executive (NACE). [Ref. 21: p. 65]

D. DEVELOPMENT

The Joint Deployment System is being developed in five stages. The Baseline Stage has been completed and JDS now provides service to the joint deployment community. The Initial Operational Capability (IOC) for the second stage, which includes limited on-line update and query features, distributed processing support via the Remote User's Package (RUP), and data base backup at REDCOM, was achieved December 1982. The third stage incorporates long-term requirements definition and validation. These additional requirements will support the Crisis Action System (CAS) and will emphasize such things as multi-plan support and no-plan support. The fourth stage is Full Operational Capability (FOC) and the IOC is presently December 1985. Since JDS is the center of the Conventional Planning and Execution (CPE) functional family of the WWMCCS ADP program, the fifth stage, Post-FOC, will detail the JDS integration into the WIS modernization program. [Ref. 10: p. 78]

The JDS data base presently contains 108 record types chained in logical record relationships in the Honeywell Integrated Data Store (IDS) structure. The data includes information on forces, nonunit personnel and cargo, movement, and transportation. The JDS is a conglomeration of 375 application programs and subprograms which maintain and manipulate the deployment data base. The majority of the JDS software works on menu-selection and pre-defined display screens. Although the entire data base is resident at the JDA, various deployment community members will maintain separate data bases to satisfy unique command requirements and command and control functions. Each of these sites will also maintain a Data Base Management System (DBMS) and local access to the main data base. These distributed data bases will be subsets of the master data base and will be maintained concurrently with the master by near-simultaneous (within five minutes) distribution of data transactions. This distribution will significantly reduce WIN activity and network performance degradation associated with large data transfers. The distributed data bases will also enhance JDS survivability by providing multiple backup locations for JDA functions. [Ref. 10: p. 25]

E. FUNCTIONS

One of the major JDS functions is to provide a bridge between deliberate planning and time sensitive planning and execution. The two systems utilized during these procedures are the Joint Operational Planning System (JOPS) and the Unit Status and Identification Report (UNITREP) System. JOPS establishes procedures for planning and executing deployments during peacetime and crisis situations as directed by JCS; the UNITREP System contains the location and identification of actual military units needed during

the planning and execution phases of deployment. The JDS supplies the necessary link between these two systems by maintaining an up-to-date deployment data base. [Ref. 10: p. 9] Figure 3.2 graphically illustrates the JDS connection between deliberate planning and time-sensitive planning and execution. [Ref. 10: p. 10]

During the deliberate planning phase, Time-Phased Force Deployment Data (TPFDD) files are developed for a specific Operation Plan (OPLAN) using JOPS and UNITREP. The initial data is collected from supported commanders and service requirements. The JCA holds a two-phase conference for refinement of the data and then the TPFDD is incorporated into the JDS data base for that specific OPLAN. This method provides the primary source of input into the JDS. Some problems with these procedures are the time-consuming conferences and reviews and the manual manipulation of the data. [Ref. 10: p. 12]

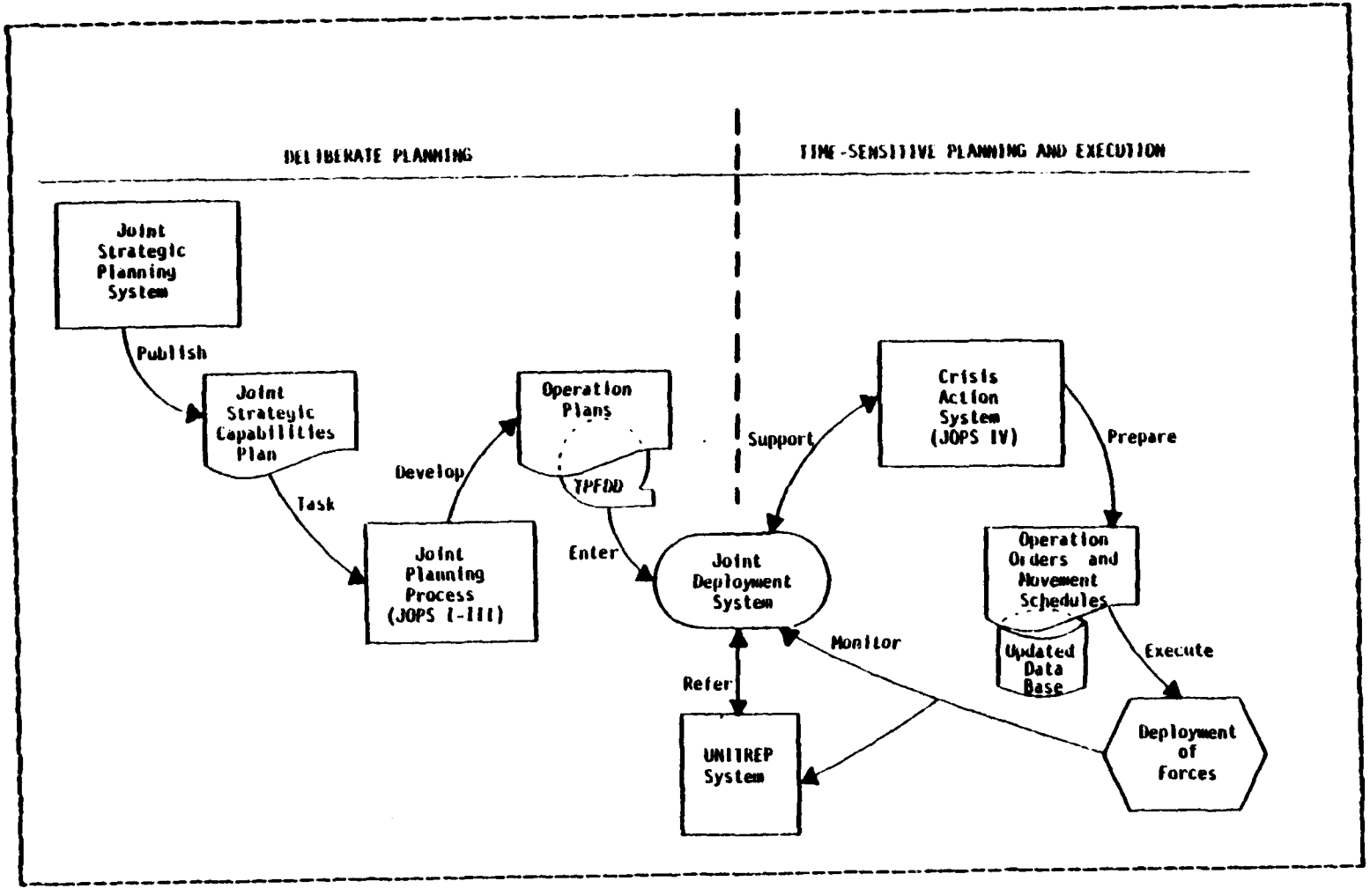


Figure 3.2 Overview of Military Planning and Deployment.

P. REMOTE USER'S PACKAGE

Since the majority of JDS users are remote and the File Transfer Service (FTS) on WIN has proven to be slow and unreliable, the Joint Deployment Agency developed the Remote User's Package (RUP) to offset some of these problems. The RUP is installed at selected WIN sites to alleviate some of the network overloading caused by large data transfers. When utilizing the Remote User's Package, no direct connection to the JDA host via WIN TELNET is required to access the data base. [Ref. 21: p. 26] Since the RUP permits users to input update and query transactions via their own Time-Sharing System (TSS) and the data base is then accessed through WIN, users experience a significant degradation of own TSS response time. The JDS Remote User's Package includes an Interface Processor (JDSIP), an Update Processor (JDSUP), a time-sharing package, and a batch update capability. [Ref. 19: p. 7]

The JDSIP provides the necessary communications protocol for transaction processing between two WIN sites. The sending site JDSIP breaks bulk files into individual transactions, then the receiving site JDSIP accepts each transaction and passes it to the JDS if a WIN connection is available or holds the transaction until a connection is made. An acknowledgement is necessary from the receiver before the next transaction (packet) is sent. The Remote User's Package essentially transforms the WWMCCS Intercomputer Network into a transaction processing system, as was the original design goal for WIN. The capability now exists for transaction update processing between two WIN sites in near-real time without dependence on a WIN connection to the JDS. [Ref. 19: p. 9]

The JDSIP of the receiving site forwards the transactions to the JDS Update Processor (JDSUP) for individual inclusion into the data base. The JDSUP is capable of receiving input transactions from the time-sharing or batch system, WIN via the JDSIP and FTS capability, and AUTODIN via the NACE processors. The Update Processor provides dynamic recovery check points during processing without task interruption. If necessary, transaction processing recovery is achieved after a communications interruption using these checkpoints, thereby no longer requiring the complete reinitialization of the task. [Ref. 19: p. 9]

Although JDA-generated software has greatly improved JDS performance, particularly in the WIN arena, additional improvements are necessary. JDS should be supported by software which requires a minimum amount of training and skills due to the computer experience of most users; for instance, JCS action officers. Users have recommended the information displays be modified to remove the time-frame distinction of 'deliberate' or 'crisis' planning. Although the data is now maintained quarterly by the Command and Control Technical Center (CCTC), part of DCA, the JDS deployment data base should move towards real-time maintenance to constantly provide a current deployment situation data base resident at JDA. [Ref. 10: p. 13]

Additional areas for general system improvement include:

(1) revising man-machine interfaces for simplification

(2) aggregating information for senior level managers on general JDS capabilities

(3) insuring more accurate and timely data collection

(4) developing standard data definitions

(5) enhancing the recovery and backup facilities

[Ref. 10: p. 19]

IV. WWMCCS/JDS PERFORMANCE

As previously discussed, the information flow between the NCA and military forces depends upon a reliable, secure, and survivable intercomputer network. The WWMCCS Intercomputer Network (WIN) was designed to provide exchange of information through computer-to-computer and remote terminal-to-computer processing using distributed data base concepts and workload sharing techniques. [Ref. 5: p. 42] WWMCCS evolved through the early years as services developed hardware and software to meet unique requirements. Based on the evolutionary approach to systems development, WWMCCS should evolve through requirements specifications as opposed to the traditional system acquisition approach. This theory is supported by a lack of specific C3 system criteria; poorly understood C3 systems concepts; language barriers between the policy makers, planners, and commanders; and the nebulous framework for C3 systems evaluation. [Ref. 5: p. 16] There are numerous systems other than C3 systems which suffer from one or more of the problems mentioned. For instance, any highly specialized system will likely experience barriers among technologists and users.

As proven with the early WWMCCS, allowing users to develop small, unique systems independently, precludes the integration of these systems into a responsive, larger system. Obviously, interoperability was not the primary concern for these individual funding efforts. Twenty years later, WWMCCS remains somewhat fragmented due to the absence of a centralized, long-range plan for the management and budget control of WWMCCS and the Defense programs affecting WWMCCS. With the WWMCCS Information System (WIS), a Joint Program Manager (JPM) Office was established to provide

centralized management for all aspects of the WWMCCS modernization program.

A. SOFTWARE

The computer operating system utilized with the Honeywell equipment is the General Comprehensive Operating System (GCOS) designed by Honeywell. Honeywell also distributes this operating system to civilian customers but the Command and Control Technical Center must extensively modify each GCOS release for security additions and unique WWMCCS Software so the GCOS used within the WWMCCS community is consistently several years behind the current civilian version. GCOS was developed to support a single-site and batch-oriented user community and has proven very successful in such situations. Present day C3 system requirements however, demand an online interactive processing capability. While modifications to the Honeywell hardware and software have improved performance, the basic circuitry is designed for batch processing and optimal performance will not be achieved in an online interactive environment.

With any large data base system, a Data Base Management System (DBMS) will be developed to allow easy retrieval and updating of the data base. Generally, these management systems are user-friendly and require minimal technical expertise for successful use. The DBMS used with WWMCCS is the WWMCCS Data Management System (WWDMS). Since WWDMS resides on the Honeywell equipment, it relies on the GCOS operating system; therefore WWDMS was designed around a batch-oriented architecture. WWDMS uses GCOS to access files for retrievals and updates. Because of the inefficiencies of the military version of GCOS in transferring data in and out of primary memory, the performance of WWDMS is adversely affected. [Ref. 5: p. 25]

Reports on the user-friendly aspect of WWDMS have not been favorable. For the most part, the WWDMS language is oriented towards the more technical personnel and is considered too detailed for the average WWMCCS user with minimum computer training. Consequently, users are not likely to pursue the management system capabilities beyond standard procedures and WWDMS' full facilities remained unused. For the community to explcit the systems and capabilities available in WWMCCS, a user-friendly and responsive DBMS is a necessity. Since the concepts of a distributed databse management system are new, a reliable query language could suffice during the development interim. It should require minimum computer experience and a minimum amount of special training.

The need for a Multi-Level Security system will not be satisfied utilizing the the current WWMCCS Honeywell equipment since this design incorporates only two machine states, or rings. The Master state accomplishes the kernel functions of the operating system, password validation and data requests, as well as the functions for scheduling and allocation of resources. The second state is for user applications programs, referred to as the Slave state. **[Ref. 5: p. 29]**

Since the security protection procedures, all system software, and the resource allocation procedures reside in the same ring, access to the specified ring area is common to all users with access to any one section of that ring. The current theory is that, under this scheme, any good systems programmer should be able to penetrate the kernel section and gain access to all passwords and security checking procedures.

Security alternatives to a MLS system are dedicated computers, scheduled operations, and system-high security operations. With dedicated computers, a separate computer

is required for each security level and individual data bases are required for each application requirement within the different security levels. The scheduled operations method insures all data per security level is processed at separate times. This restricts users of different security levels to computer availability. The most difficult aspect to this method of secure processing is the sanitization necessary between security level processing periods. The entire system environment must be modified, both the machine and physical facility. In addition, communications lines must be broken, disk packs must be exchanged for the different security levels, and main memory cleared. This procedure averages one to two hours to complete. [Ref. 5: p. 28]

The third alternative, system-high security operations, is primarily used throughout the WWMCCS community. With system-high operations, all personnel, physical space, and equipment must be approved for the highest security level of the information being processed. The biggest disadvantage to this method is the restriction it places on the sharing of secure computer resources. In addition, this method becomes costly in terms of physical security and personnel clearances. The system-high security approach, if implemented correctly, will satisfy security level requirements but does not address the need-to-know issue. [Ref. 5: p. 28]

B. HARDWARE

The availability of an electric power source greatly affects the reliability and survivability of a computer network such as the WWMCCS Intercomputer Network (WIN). For the current WIN, there exists no standard criteria for the availability of electric power. If electric power is

disrupted or the air-conditioning damaged, data processing capabilities are totally lost or, at a minimum, severely degraded. Only a few WIN sites have a reliable backup power source or redundant computer system. The National Military Command Center (NMCC) maintains two independent power sources for its computer system. This system affords protection against various local power blackouts and irregularities in the commercial power system. [Ref. 5: p. 29] The NMCC also maintains a totally redundant computer system, hardware and software, located at the Alternate National Military Command Center (ANMCC), which has an internal power generating capability. In early WWMCCS years, the ANMCC was considered hardened and fully self-supporting, but the alternate site is no longer considered hardened against the current threat. A few other large WWMCCS sites utilizing commercial power are also armed with an internal power generating capability, for instance, the North American Air Defense Command (NORAD) and the Strategic Air Command (SAC). Most other WWMCCS sites have no reliable backup power source.

Presently the NMCC has, of course, the most viable alternate computer system -- both redundant and remote. Other sites maintain redundant data bases but usually in close proximity. For example, the Joint Deployment Agency maintains a backup JDS data base at the Readiness Command (REDCOM) but which is physically located at the same facility.

C. IVY LEAGUE 82

During the period 1 March to 5 March 1982, the JCS conducted a WWMCCS exercise, IVY LEAGUE 82. The exercise was designed to evaluate defense operations run from the NMCC at the Pentagon, then relocated to the alternate

command center, the ANMCC. As the exercise progressed, WIN performance dropped and response times reached an unacceptable level. A DCA/CCTC sponsored IVY LEAGUE Analysis Task Force was organized to analyze the performance of the WWMCCS ADP system and network, with concentration on the particular problems encountered during the IVY LEAGUE exercise. [Ref. 22: p. 1-1]

The Task Force focused its analysis on the four major sites where the slowdown condition was most prevalent: the NMCC Readiness System, the ANMCC, REDCOM, and the JDA. These four sites were not all the WIN nodes participating in the exercise, but it was felt these sites were indicative of overall WIN performance during IVY LEAGUE 82. Information was collected from on-site exercise personnel, manual logs updated throughout the exercise, computer generated listings, and WWMCCS computer system console logs from the participating sites. [Ref. 22: p. v]

The IVY LEAGUE Task Force revealed several major factors contributing to the WIN degradation:

(1) excessive communications processor loading
(2) communications subnetwork fragmentation
(3) host computer resource contention
(4) software resource contention
(5) management of computer operations

Each of these will be discussed in the following sections with their impact on JDS performance.

D. COMMUNICATIONS PROCESSOR LOADING

The successful operation of the WIN network depends on an unconstrained flow of data between the computer system and the network. A communications processor is used on the network to coordinate inputs from remote terminals and send them to the host system; it also receives outputs from the

computer system and sends them to the correct user. The communications processor handles the connection from the host computer system to the network. The Honeywell Datanet 355 (DN 355) is the communications processor used throughout the WWMCCS community.

The design of the Datanet requires sufficient available memory to process message traffic; otherwise the Datanet may restrict the flow of traffic from the host to the network and from remote sites to the host through unsatisfactory terminal response time and slow file transfers. The block of memory allocated for message processing is subdivided into sections called buffers. Buffer size is dependent on the type and number of connections to the Datanet. The greater the number of connections, the lower the available memory and the lower the buffer size. WIN connections to the Datanet must contend for buffer space with remote processors, AUTODIN connections, and the local terminals. [Ref. 22: p. 2-1]

During IVY LEAGUE 82, when the Datanet became overloaded, users experienced up to ten second pauses for system response. Some of this was attributable to Datanet overconfiguration -- too many connections to one Datanet. At JDA, all 115 local terminals and the WIN connection were served by the one Datanet. In some cases, several terminals shared one line into the communications processor which further hindered terminal response time. In addition to the terminal overloading, this same Datanet also served the AUTODIN interface at all four sites reviewed. [Ref. 22: p. 2-1] With this Datanet configuration, any terminal disconnect from the system or any Datanet failure affects all connected terminals, both local and remote. Considering the large number of terminals connected, the chance of a Datanet failure or system reinitialization (reboot) to clear terminal or WIN problems is extremely high. Figure 4.1

graphically depicts user-dependence on the DN 355/Host link. [Ref. 8: p. 3]

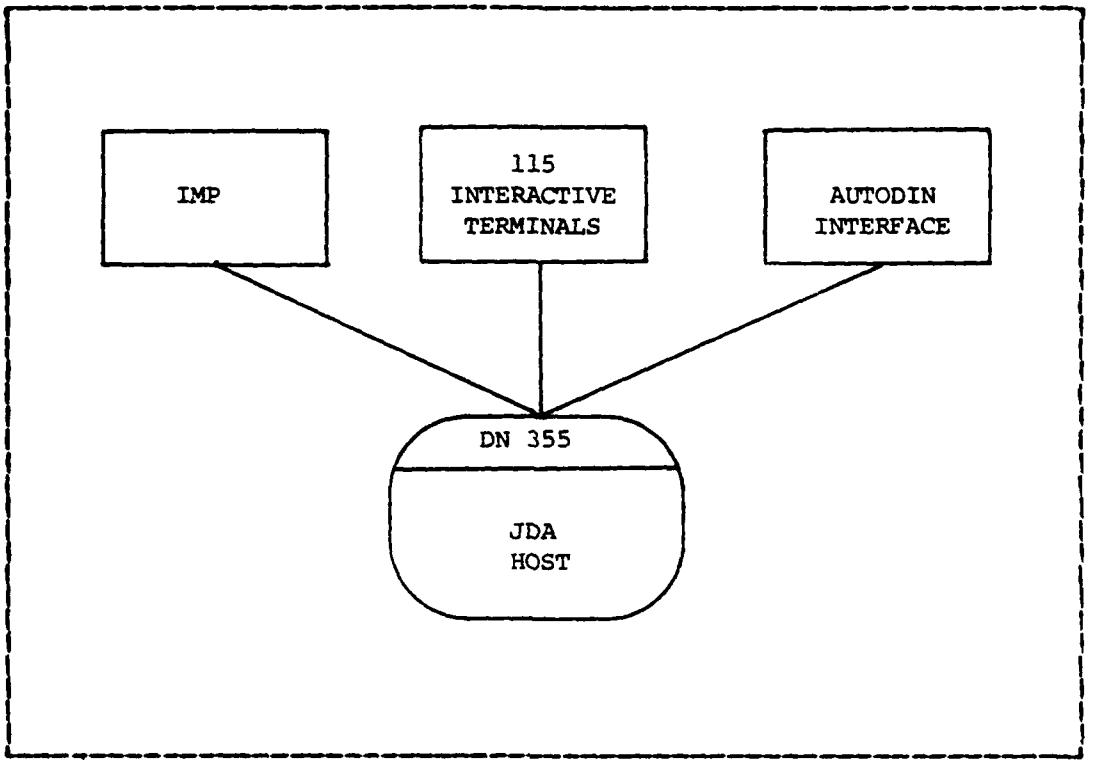


Figure 4.1 JDA Configuration.

During periods of particularly bad performance in IVY LEAGUE 82, computer data dumps were taken from the REDCOM Datanet. JDA Datanet dumps were not available, but the REDCOM configuration was considered similar to that of JDA with 139 local terminals connected to the one Datanet. Data retrieved revealed 4,490 data transfer requests denied during a 17-hour period because of insufficient buffer space. During a separate 22-hour period, an additional 4,651 data transfers were denied due to lack of buffer space. These numbers only reflect Datanet denials, local Interface Message Processor (IMP) and terminal malfunctions

may also have occurred. During IVY LEAGUE 82, the JDA host computer received an average of 150,000 transactions per day. Specifically, on 2 March, JDA processed 252,864 transactions and 87,417 transactions were processed on 4 March. [Ref. 22: p. 2-2]

Another hinderance to Datanet performance was operator reboots of the Datanet. Operations would frequently reinitialize the Datanet in an attempt to free blocked terminals or solve WIN problems and various other abnormalities occurring in the network. [Ref. 22: p. 2-1] Although the specific impact of these Datanet restarts were not analyzed, they obviously affected WIN performance. For instance, the Joint Deployment System tranfers TPFDD files and TPFDD file changes to remote sites through the WIN FTS. If a Datanet reboot occurs during this time, the file transfer must be recovered. Previous to the development of the Remote User's Package (RUP), transaction recovery meant file transfer reinitialization. Now, the JDS Update Processor (JDSUP) dynamically generates checkpoints throughout the transfer to allow file transfer recovery at the point of disconnection.

The WWMCCS community employs Datanet performance monitoring software to warn of possible Datanet overload. This monitoring software requires approximately 2,500 words of memory which further reduces the Datanet memory available for message processing buffers. Consequently, at all four sites included in the analysis, the monitoring software was not in execution. [Ref. 22: p. 2-1]

E. NETWORK FRAGMENTATION

As discussed in the previous section, the WWMCCS network is very susceptible to interruptions occuring within the lines of communications. Any network configuration changes, component outages, or circuit failures will cause

fragmentation of the network into subnetworks, thus degrading performance. [Ref. 22: p. 3-1] Each WWMCCS host computer involved in the WWMCCS Intercomputer Network is linked to a Honeywell minicomputer called an Interface Message Processor (IMP), and the various IMPs are then interconnected.

During IVY LEAGUE 82, the Network Operations Center (NOC) and DCA Operations Center (DCAOC) were relocated to the alternate command center, the ANMCC. To provide continued support for these nodes on the WIN subnetwork, the master IMP, normally at the Pentagon, was logically reconfigured to the backup facility at the Command and Control Technical Center (CCTC), Reston. Changes were necessary within the WIN subnetwork due to the backup IMP's limitations and circuit availability. The major modification was the deletion of the link from the master IMP to the IMP at Headquarters, Atlantic Command. As the exercise progressed, it became evident that the loss of this one particular link proved to be a major factor in network fragmentation. During these periods of fragmentation, the exchange of data between WIN sites was totally disrupted. [Ref. 22: p. 3-2]

Although the IMP and circuit outages were usually short, these, coupled with the major configuration changes, severely degraded WIN performance. For instance on 2 March, 88 circuit outages occured for a total of 5.13 hours down-time. Later in the exercise on 4 March, a sum loss of 7.72 hours was felt during 138 circuit outages. For the entire IVY LEAGUE 82 exercise, 476 line outages occured with 65 extending over 10 minutes, 22 of these outages were the result of required cryptographic key changes. Key changes were a frequent cause for circuits displaced from normal activities. IMP outages for the exercise totaled 334 with 52 lasting over 10 minutes: 77 at 6.63 hours on 2 March and 82 at 7.62 hours on 4 March. [Ref. 22: p. 3-6]

F. RESOURCE CONTENTION

During IVY LEAGUE 82, numerous cases of host resource misuse occurred in areas such as primary memory allocation, job priority assignment, and improper implementation of WIN software. These conflicts severely limited the host system performance. The Analysis Task Force studied these problems at the NMCC Readiness and ANMCC computer systems only, but it was felt similar situations existed at numerous other WWMCCS sites. [Ref. 22: p. 4-1]

The NMCC WWMCCS site is segregated into two distinct computer systems: Readiness and Support. The Readiness System is designed for the operation of WWMCCS standard software and other site-unique software that has previously been tested and is now in production. The NMCC Support System is an identical configuration to the Readiness system and exists for the development and testing of new software. Only the Readiness System participates in JCS exercises as the Support System continues to support daily operations. Priorities fall so that the Support System may be sacrificed to maintain the performance of the Readiness System.

With only fully operational software allowed on the NMCC Readiness System, the percentage of aborted jobs is expected to be small. During the exercise, the amount of computer resources expended on jobs which ultimately aborted was unacceptably high. Some aborts were due to magnetic tape and various other hardware problems, but an undesirable number were caused by software still in the developmental stage. [Ref. 22: p. 4-2] Prior to a new WWMCCS software release, the temptation for programmers to use the Readiness System as a testbed for application system modifications is high. The response time is decidedly better on the Readiness System because of decreased aborts and code optimization. Guidelines for testing state all systems resident

on the Readiness system to be tested and/or modified will be transferred to the Support System. After verification with the new WWMCCS software, the modified system will then replace the old system on the Readiness computer. The idea, of course, is to preserve the Readiness computer in both time and space requirements for crisis/exercise support and employ a second system for the heavy processing and the usually large space consumption of software development.

Both systems studied, the NMCC Readiness and the ANMCC system, suffered from a lack of available memory for processing. In particular, on 2 March memory shortages severely constrained processing capabilities for a five hour period. Under the current WWMCCS ADP, it is possible to dynamically reconfigure a system without completely bringing it off-line; for example, allowing the addition of memory to the host computer system during an exercise. [Ref. 22: p. 4-1] Although infrequently done, memory may be acquired from the NMCC Support System to improve the performance of the Readiness System.

A standard WWMCCS program size is approximately 60K (60 x 1024 bytes). Any one application program requiring more than 60K or a large amount of CPU time, should be remodeled to include code optimization and some method of memory overlays or paging. [Ref. 22: p. 4-1]

In addition to large memory utilization, numerous jobs with high priorities running simultaneously will affect system performance. Honeywell supports an urgency system for determining job priorities -- urgencies may vary from zero to 63. Typically, urgencies of 30 and below are used for user application programs; for example, routine batch and TSS jobs are assigned an urgency of 5. Urgencies above 30 are reserved for system software applications and special production runs. Urgencies higher than 50 support system programs such as TLCF, FTS, and other WIN software. [Ref. 22: p. 4-2]

Statistics show approximately thirty percent of all activities processed on the ANMCC computer system during the exercise had urgency levels greater than or equal to the urgency levels of system functions. Software such as TSS and WIN have urgencies from 50 to 60 to allow primary access to the processor. During IVY LEAGUE 82, this software was competing with user application software for computer resources because of unjustified high user application urgencies. [Ref. 22: p. 4-1]

The WWMCCS system console operator has the ability to override system prescribed urgencies. This is usually accomplished on a case by case basis for ad-hoc production runs. Any system requiring a large block of memory, substantial CPU time, or lengthy input/output processing will normally be awarded a lower urgency, causing it to remain in the system a relatively longer length of time. When the urgencies of these systems are bumped to higher levels, whether justified or not, they compete with system software, usually large time-consuming systems themselves and the 'molasses condition' occurs -- total system slowdown. An incrdinate amount of automated bookkeeping is necessary for proper resource availability and the processor becomes overloaded. When this condition occurs, known as thrashing, the effectiveness of the Honeywell urgency system drops to zero.

The cumulative affect of all the above mentioned situations equals increased user response time and user frustration. During normal NMCC operations, TSS response time averages five to seven seconds; during heavy usage, exercises or crises, response time increases incrementally by approximately three seconds until total system slowdown occurs.

WIN software is not always the 'victim' of poor WIN performance. Some software, both systems software and application systems, contribute to the increase in host system processing requirements. When these requirements exceed system capabilities, support of local and network operation decreases.

Some of the WIN system software particularly affected by degraded network performance includes:

(1) Teleconferencing (TLCF) System

(2) File Transfer Service (FTS)

(3) Telecommunciations program (TELNET). [Ref. 22: p. 6-1]

The Teleconferencing capability in WIN allows users to rejoin the conference and request a transcript file of actions since that site's last log-on. These files are spooled to the printer at a high urgency for speedy printing. During IVY LEAGUE 82, the large number of transcript file requests severely impacted the performance of the system hosting the teleconference.

The File Transfer Service employed in the WIN utilizes a dynamic memory management scheme to maintain an available memory level between the minimum and maximum guidelines. The management system constantly allocates and deallocates sections of memory as small as 1K to sustain an acceptable memory level. This continuous processing requirement places a heavy load on the host processor. Also, during a file transfer, FTS reads and writes one Little Link (LLINK) of data at a time, 320 words. This limits possible transfer rates and FTS effectiveness. [Ref. 22: p. 6-1]

TELNET uses software similar to the FTS memory management software. Although this imposes additional loading on the processing system, the contribution to system loading is not as significant as FTS or TLCF. [Ref. 22: p. 6-1]

G. JDS RESOURCE CONTENTION

Large software applications used over the WWMCCS network, such as the Joint Deployment System, need to be concerned about resource requirements and operational efficiency. Since such a wide degree of diversity exists among application systems, no guidelines for standardization of new WWMCCS software have been established; therefore, these issues are left to the developing agency. For instance, the Joint Deployment System maintains two interactive subsystems, the JDSIP and JDSUP as part of the Remote User's Package (RUP). The Analysis Task Force contends these two subsystems fail to take the best advantage of the standard WWMCCS software features and consequently generate substantial overhead for the processor. After analysis of IVY LEAGUE 82, the need was evident to redesign portions of the JDS software to insure more efficient processing and overhead minimization. [Ref. 22: p. 6-3]

The operation of the JDSIP caused noticable degradation during the exercise. The Interface Processor subsystem requires 28K to process and runs with an urgency of 51. The JDSIP will remain in memory as long as it is processing transactions. When the processor is not required, i.e., no transactions to be processed, the JDSIP will place itself in a 'sleep state' -- degrading its urgency to zero which immediately allows it to be swapped out of the system at the next memory allocation request. Actually, this should be very efficient use of memory, or at least 28K. The problem arises in waking up the JDSIP. Since the subsystem has no means of determining when the next transaction will be received, the JDSIP periodically, about every two to three seconds, resets its urgency back to 51 which returns it to memory where it can check for transactions to be processed. If no transactions are waiting, the urgency is returned to zero and the cycle repeats. [Ref. 22: p. 6-3]

This scheme is at its worst when JDS is rarely used on a given system. The JDSIP simply fluctuates from mass storage to primary memory with no advantage. This swapping back and forth creates unnecessary overhead processing and can seriously degrade network performance. Case in point: on 1 March, during IVY LEAGUE 82, the JDSIP was swapped a total of 412 times in an eight-minute period, from 1355 to 1403. [Ref. 22: p. 6-3]

The JDS Update Processor (JDSUP) poses a similar situation. The JDSUP requires only 9K to process and runs at an urgency of 55. During certain processing periods, the JDSUP must request a single block of 50K of memory. When this request enters the system, the system will immediately rearrange its memory to accommodate the request from such a high priority job. Usually, a system interruption is evident. After the JDSUP has completed that process, the 50K is returned to memory; however, the JDSUP in general immediately asks for another single block of 50K to continue processing. [Ref. 22: p. 6-3]

The allocation and deallocation of this 50K of memory proved to be detrimental during the IVY LEAGUE exercise. On 2 March, JDSUP requested 50K at 0120, released the memory at 0122, and requested another 50K block at 0125. This cycle of request-release-request was repeated during the 0330-0340 time period that same day. [Ref. 22: p. 6-3]

H. MANAGEMENT OF COMPUTER OPERATIONS

During IVY LEAGUE 82, it became evident that hardware and software problems were not entirely responsible for the C3 system degradation. The overall management and control of the network and host system also contributed to deficient performance.

As part of the normal operations of all WIN sites, hardware such as the host computer system, the Datanet, and the IMPs are reinitialized in an attempt to solve various problems. These reboots interrupt network performance and can impact local user operations. In addition to unexpected down time and reboots, scheduled outages occur at all sites. The WWMCCS community has no standard guidelines for the scheduling of these outages. Frequently, these unscheduled downtimes are not justified; for instance, during the exercise, a Datanet was rebooted to allow a single user access to a particular system for a local processing requirement. This reboot affected all users on that subnetwork.

On 3 March, the ANMCC discontinued service to remote users because of an apparent memory shortage problem. According to VIDEO, an online display system which allows monitoring of system status, minimum work was being processed because of a lack of available memory. The after exercise analysis however, revealed approximately 150K of memory available during that time frame. The discrepancy occurred due to improper use of the VIDEO system. This system is designed to provide an instantaneous picture of system resources. The system was likely restructuring memory to accommodate the increased workload when the decision was made to detach all remote users. [Ref. 22: p. 5-2]

Another operational contribution to poor network performance occurred when FTS was used to transfer files around within the same site, as opposed to using a COPY utility. Transferring a file with sending and receiving sites specified as the same site, sends the file to the local IMP which immediately returns the file to the same host. During IVY LEAGUE 82, exercise statistics showed that 34% of all file transfers at the NMCC were same-site transfers, as were 67% of Military Airlift Command (MAC) transfers and 83% at the WWMCCS site supporting the Commander-in-Chief, Naval Forces

Europe. [Ref. 22: p. 5-3] This type of functional misuse wastes host system resources and contributes to WIN loading.

V. RECOMMENDATIONS AND CONCLUSIONS

When the current WWMCCS/WIN management problems are addressed during the modernization phase, network perfcrmance should improve. This will decrease user frustration, especially during high volume times, and increase user activity on the system. This increase in volume in turn, may affect system performance and, with greater user participation comes additional site-unique software. Site-unique applications are created due to deficiencies within the system which will always exist in a system as large as WWMCCS. The WIS modernization plan does not propose to eliminate this unique category of WWMCCS software, just minimize its proportion to standard software.

A. SOFTWARE

The WIS modernization plan includes a new operating system release, GCOS 8.0, and a modified Honeywell mainframe, the H6000 Distributed Processing System (DPS).

The major software modifications include:

(1) improved data management and timesharing processing

(2) DPS software written in a high order language which facilitates maintenance and modifications

(3) increased number of timesharing users from 200 to 600

(4) increased number of concurrent processes from 64 to 511 [Ref. 23]

Not mentioned in the WIS modernization plan is any justification that this increase in possible user activity will not further degrade system performance. Although a new

processor is under consideration, the H6000 DPS modification, a significant increase in processing capability is already critical to maintain availability of present WWMCCS software. Increasing the number of time sharing users three-fold will quickly consume any available processing time.

The WWMCCS modernization plan also includes the DM4 software package for better file management, allowing different file structures for files in the same data base, and an enhanced DBMS, the Integrated Data Store II (IDS II). With the current IDS I, the progammer is not independent of the data base -- one of the fundamental requirements of a Data Base Management System. When using IDS I, the user must know the data base layout, referred to as the schema, and must include various system routines to successfully update the data base. IDS II will be more of a true DBMS, allowing user independence from the data base schema.

With a true DBMS, more users are likely to pursue information contained within the system, thus increasing user retrievals from remote sites, i.e., retrieval requests from the JDS, and increasing data transfers on WIN. Again, the WIS modernization plan lacks an apparent knowledge of how to handle this increase in activity.

Although the basic software design of the WWMCCS equipment is inadequate for a Multi-Level Security (MLS) system, there has been a proposal using hardware modifications. Honeywell has developed a system, the Honeywell Secure Communications Processor (SCOMP), which runs on the Honeywell Level 6 minicomputer and is billed as a MLS system. SCOMP utilizes four rings of protection with the kernel residing in Ring 0 and the least priviledged ring, Ring 3, belonging to the users. But SCOMP also modifies the hardware by supplying a hardware segmentation capability for dividing main memory into distinct logical (not physical)

areas. This should allow access checking per segment for read/write priviledges, thus maintaining controlled software sharing among many users. [Ref. 24: p. 4]

While SCOMP has not been fully validated by the DOD Computer Security Center, part of the National Security Agency (NSA), it is considered a large step towards the secure, time-shared computer resources needed in communities such as the WWMCCS community. In December 1981, the security center published a Product Evaluation Bulletin specifying that SCOMP "... should be considered an acceptable candidate for a wide range of minicomputer applications which require an enhanced architecture to support secure processing requirements." [Ref. 25]

Another emerging alternative is the BLACKER Technology. BLACKER will supply end-to-end encryption through the BLACKER Terminal Access System (TAS). This TAS is a PDP 11/70 or PDP 11/34 and acts as a buffer between the network and host computers for security verification. Upon log-on, each user will be assigned a one time key for the life of the terminal session. These keys will be checked and verified before access to each data base is allowed. They will also be used to control inadvertent misrouting of data, referred to as spillage. [Ref. 26: p. 6]

The main idea behind the BLACKER prototype is to alleviate the burden of numerous passwords for each user per each host computer. Passwords are no longer considered secure for some classification levels because they must be stored within the computer system and users frequently violate security procedures by writing them down. One of the most viable alternatives proposed has been the use of magnetic strip identification badges and electronic badge readers. This system would allow for minimum manual intervention. [Ref. 26: p. 17]

A MLS system would allow the Joint Deployment Agency to control access to various capabilities in specific OPLANs. Presently, all host computers and personnel must be cleared to the highest security level of any piece of data contained in the OPLAN.

Functioning without a MLS system, full utilization of WWMCCS resources is improbable and the sharing of computer resources over the network is restricted. During the interim between the present security procedures and the eventual development of a MLS system for WWMCCS, the WIS JPM becomes the central WWMCCS security officer to standardize physical security procedures and set guidelines on the handling of different security levels on the same machine.

B. HARDWARE

The WIS modernization plan does not address the issue of redundant power supplies. The vulnerability of computer hardware to electric power for operations and support, i.e., air conditioning, is immense. With very few WWMCCS nodes having a reliable backup power source, the network should not be considered survivable.

Included in the near-term WIS modernization program is the procurement of the Honeywell 6000 Distributed Processing System (DPS) modification. The H6000 DPS offers major hardware and software improvements over the H6060 and H6080 equipment currently used in the WWMCCS community. Major hardware changes include:

(1) 70% to 90% increased processing speed

(2) space, power, and air-conditioning requirement reductions

(3) three-ring architecture for MLS system possibility [Ref. 23]

The Honeywell mainframes presently used are fast approaching the age of computer antiquity. The largest problem centers around the Honeywell architecture which was not designed to support an online, interactive environment. When hardware replacement is considered, the WWMCCS host computers should be replaced with computer systems designed to support a real-time, online, interactive environment.

The changing requirements for network software, moving this software onto the Datanet processors, and advancements in computer technology have all reduced the mainframe requirements for most WWMCCS sites. For hardware acquisition, WWMCCS sites will consider a series of minicomputers, for instance the Honeywell Level 6 minicomputers, versus one large machine. Of course, each site would be unique in configuration but a typical WWMCCS site could employ one Level 6 for each of the following functions: the AUTODIN message processing, the WIN connection to include handling TLCF support, the ADPIO functions, and all resident data bases and local processing requirements.

C. COMMUNICATIONS PROCESSOR

The WWMCCS community has communications processor monitoring software which consumes 2,500 words of Datanet memory when implemented but can supply valuable information on Datanet overload situations. The implementation of this monitoring software for the Datanet is not a requirement for WIN sites, but each site should perform a trade-off analysis on memory required and information received. The statistical output from the monitoring software could reduce Datanet reboots by notifying operators of potential weaknesses in the system; i.e., running out of buffer space for message processing or the number of transfer denials exceeding an acceptable level. If memory space cannot be

supplied during a crisis/exercise situation for the monitoring software, controlled simulations using the Datanet monitoring software should be implemented to forecast potentially threatening process combinations to the Datanet.

A set of standard system guidelines should be developed for use at all WIN sites to establish acceptable criteria for Datanet reboots. Frequent rebooting as a first try at solving a network problem should be discouraged.

Also, a WIN software validation package should be developed to prohibit file transfers within the same site. Included should be installation checks to insure WWMCCS Standard System Software is installed properly and site options are set at the prescribed level. [Ref. 22: p. 7-4]

The Datanet overconfiguration problem, i.e., 115 terminals linked to one Datanet at JDA, lends itself to two recommendations. The first solution is simple but rather expensive -- procure more Honeywell Datanet 355 processors. Ideally, this would allow one Datanet to be dedicated to that site's WIN connection. This configuration would reduce WIN problems associated with operator reboots of the Datanet to solve non-WIN problems. [Ref. 22: p. 2-2] With additional Datanets, user load could be better distributed and Datanet failures would have less impact on the site performance. At a minimum, sites should avoid linking high volume connections such as WIN, AUTODIN, and the JCS ADP Liason Officer (ADPLO) terminals on the same Datanet. In addition, sites should adhere to the standard WWMCCS loading levels for the Datanet as directed by the WWMCCS ADP Advisory Memorandum (WAAM).

The second recommendation is to eliminate the Honeywell communications processor equipment and transfer these functions either to another vendor communications processor or to a minicomputer, such as the Honeywell Level 6 minicomputer. The Honeywell Datanet 355 is limited in a memory

size which is no longer sufficient for the normal message processing capacity at large WIN sites. Using the Level 6 minicomputer in series would alleviate the memory problems and provide additional processing capabilities.

D. NETWORK FRAGMENTATION

To prevent the reoccurrence of problems similar to the ones caused by the Master IMP being reconfigured during IVY LEAGUE 82, contingency plans should be devised to eliminate the drastic configuration changes as were necessary when such a targetable IMP was deleted from the network. Studies and crisis/exercise monitoring should be undertaken to predict possible circuit or IMP links which could initiate network fragmentation. [Ref. 22: p. 3-9] After identifying these areas, they should be reinforced during high volume times by redundant configuration or specific rerouting algorithms.

After the C/30 switch upgrade, part of the WWMCCS modernization plan, IMP and circuit outages should decrease. The C/30 switch will provide tandem processing of up to 300 packets per second, for a total of 900 packets being processed. Routing and rerouting will be accomplished by adaptive routing algorithms which will reroute individual packets to the shortest path. In addition, monitoring and control functions are included to provide fault isolation and hardware and software problem diagnosis.

Replacing the huge WWMCCS network with a series of Local Area Networks (LANs) will alleviate some of the degradation felt during network fragmentation. Moving the network software from the Honeywell mainframes onto the Datanets is the first step in building independent LANs. Eventually, all network software should be moved, alleviating the mainframe from any network control responsibilities. This would

remove the restriction for standard hardware for all WIN sites. With no standard hardware limitations, users could tailor the acquisition of new hardware around specific site requirements. Since all host systems will be linked through a common network, minimum compatibility problems should be experienced.

E. RESOURCE CONTENTION

One popular recommendation for the mainframe processor contention problem is the addition of another processor for the NMCC Readiness System. This additional processor would be justified during an exercise but not fully utilized during daily operations.

As opposed to procuring an additional processor, the Support System could be modified to temporarily provide the necessary hardware/software equipment during crisis/exercise situations. The main advantage to this plan is reduced swapping for CPU contention. [Ref. 22: p. 4-3] The validity of this plan is somewhat questionable. Previous to the NMCC WWMCCS computer system division into Readiness and Support systems, there was a H6080 machine with two processors. CPU contention reached a level to warrant the separation of production and development efforts, thus was born another computer system strictly for developmental efforts. Configuration now stands at two separate systems with one processor each. As mentioned in a previous section, users do not always respect the guidelines for use of these two systems. In light of user-induced problems affecting performance, stronger enforcements of implemented procedures would be more cost-effective. The recommendation for an additional processor is expensive whether the dollars are spent actually procuring another processor which will be fully utilized only about twenty-five percent of the time or

the Support System software is used for high-priority usage. During the later option, numerous software development personnel with no planned participation in a crisis/exercise environment, would be without a computer processor which greatly restricts their developmental efforts.

Also hindering processor performance is the Honeywell urgency scheme for processes. The basic idea of the Honeywell urgency scheme is acceptable. The urgency scheme needs adjusting and the implementation should be modified for tighter controls on the system console operator's ability to override the system default urgencies. Also, enhancements to prohibit application software from reaching urgencies in the WIN software level is necessary. This would discourage resource competition and improve system slowdown. One urgency system recommended included not allowing any application software to exceed an urgency of 10. Few users, mostly system programmers, would operate at urgencies of 30 to 40 and no users would exceed 40. This propcsal leaves urgencies of 40 to 63 for system software and WIN software.

A new TSS Monitor has been developed within the WWMCCS community. This monitoring software is easy to use via system console commands and no system interruption is experienced. Unfortunately, this new Monitor was not operational for IVY LEAGUE 82; but it can be utilized during the next exercise for selected small periods of time to allow a more thorough analysis of slowdown periods. [Ref. 22: p. 4-4] With the WIS modernization plan, the capability to monitor each network element is achieved through the Monitoring Centers of the DDN. DDN will also provide an automatic fault recognition and isolation for trouble spots with most reconfigurations being handled without dedicated personnel.

WIN software, such as the memory management algorithms for FTS and TELNET, should be redesigned to reduce the allocation and deallocation processing for memory. One alternative could be a minimum size of memory allowed for allocation, this would eliminate the overhead generated in the swapping of 1K.

Additionally, improved operational procedures are needed concerning teleconferencing transcript files. Options available include:

(1) spooling the printed output with a lower urgency which would force printing at less critical times

(2) allowing printing of the transcript file requests only during scheduled time periods

The resource contention problem, especially at the NMCC, is stated as a top priority of the WIS modernization plan; however, no tangible alternatives have been proposed.

F. JDS RESOURCE CONTENTION

The memory chasing problems of the JDSIP and JDSUP subsystems may be approached from several alternatives. Obviously, the amount of allocation/deallocation depends almost entirely on the idle-time of the subsystem. Studies should be conducted at each site supporting the Remote User's Package (RUP) to determine its use/idle ratio. If the JDSIP subsystem remains in memory the majority of the time, minimum overhead is generated. If the JDSIP use/idle ratio is small, significant overhead will be generated by the subsystem changing urgencies to engage placement in core and the chance of checking for transaction activities. An alternative would be the development of a small check-routine to permanently reside in primary memory. Its job would be to periodically, every two to three seconds, check for incoming transactions and change the JDSIP urgency to 51

if transactions are available for processing, at the same time changing its own urgency to zero. This would produce a sleep state similar to that of the JDSIP when inactive, only the check-routine would not leave core. When the JDSIP finished the necessry transaction processing, it would decrease its urgency to zero and change the check-routine urgency to 51. This would allow the JDSIP to be swapped to mass storage at the next memory request and the check-routine would have high priority for processor time and resume waiting for the next transaction.

Another alternative to be considered is the permanent allocation of 28K to the JDSIP. This would allow the JDSIP permanent residence in primary memory and is feasible if the host system is not memory-restricted.

The JDSUP subsystem remains in primary memory itself at 9K but periodically requires an addition 50K for processing. Part of the problem concerning the JDSUP memory allocation stems from the JDSUP requiring one single block of 50K of memory. Generally, the system must rearrange memory to create a contiguous 50K block. The easiest solution would be the permanent attachment of the 50K to the JDSUP subsystem. For a system memory-restricted at all, this alternative is impractical. A more feasible alternative would be to include 50K in the system size for the JDSUP and treat the 59K as one system. Then modify the JDSUP to reside on mass stoarge and utilize a check-routine, similar to the JDSIP, for dynamic checking of requirements. The same urgency swapping and processing schemes could be utilized.

In addition to the specific modifications to the JDS subsystem, several other measures could be taken to improve WIN resource requirements:

(1) development of standards for new application software

(2) standard criteria for resource requirements in new software

(3) code optimization and memory overlays for larger systems

(4) utilization of data compression techniques

(5) improved input/output interfaces

(6) more efficient data transaction activites

(7) elimination of large data transfers

G. CONCLUSIONS

One of the largest problems with the Defense Data Network (DDN) will be the Multi-Level Security issue. With the variety of users linked through one common network, a MLS system will be imperative.

Another DDN concern is the standard data communications protocols. These protocols should not only interface with the WWMCCS sites, but should be able to interact with NATO systems for greater interoperability. The WIS JPM presently intends to require standard protocols be written in the new DOD design language, ADA. While no ADA compiler has been fully certified as meeting all DOD standards, the step towards standard software should begin at software conception.

The WIS modernization plan will bring modern software and later hardware into the WWMCCS community. The WIS JPM strategy is to tackle the software problems in WWMCCS first and bypass the fast moving technology field of hardware until later. Not all of the WWMCCS standard software needs rewriting and by modernizing the software first, the WWMCCS network will become more adept to present day requirements.

WWMCCS ADP problems will not be solved by the WIS modernization plan or hardware changes alone. The WWMCCS computer systems are used for war-gaming and software

development but the primary intention of this C3 system surfaces during crises with the handling of message traffic. The heart of the WWMCCS ADP program must be a fast, reliable and secure transaction processing system. Faster routing algorithms must be developed and improved physical survivability is critical. Now, every node on the WWMCCS network is vulnerable to easy destruction and each node lost has a great impact on total system performance.

The WIS modernization plan with an improved DBMS, management and security procedures, and user interface is a significant start towards the remodeling of WWMCCS. The modernization is planned over a ten year period and a major concern will be maintaining service dollar support.

The Joint Deployment System will certainly benefit from the WIS modernization plan. But the areas of network management, multi-level security, and resource contention must be addressed by the modernization plan and alternatives proposed. In the meantime, the Joint Deployment Agency will continue to develop JDS-unique software to supplement WWMCCS capabilities and provide deployment information through crisis situations.

LIST OF REFERENCES

1. Morgenstern, John, "Strategic and Theater C2 Systems", Signal, November 1978, pp. 50-55.

2. Rumsfeld, Donald H., "A Command, Control and Communications Overview", Signal, pp. 35-46, May 1976.

3. Lake, Julian S., "The Many Faces of C3", Editorial, Military Electronics/Countermeasures, June 1979, p. 40.

4. Gutmann, Richard W., Problems Associated with the Worldwide Military Command and Control System (WWMCCS), U.S. General Accounting Office, 23 April 1979.

5. US General Accounting Office, Report Number LCD-80-22, Report to the Congress, the Worldwide Military Command and Control System -- Major Changes Needed In Its Automated Data Processing Management and Direction, 14 December 1979.

6. Evans, Major General Donald L., USAF, "Command and Control WWMCCS: Why the Goal is to Become More Robust", Government Executive, Volume 14, No. 6, June 1982, pp. 19-24.

7. Defense Communications Agency, Progress Report on the WWMCCS Information System (WIS) Modernization Effort, 5 January 1982.

8. WIS Joint Program Manager, Report to Congress on the WWMCCS Information System Modernization Effort, 30 July 1982.

9. Edge, Major General Robert L., USAF, "Command and Control Systems: What are They? Who Needs Them?", Signal, pp. 23-26, March 1975.

10. Joint Deployment Agency, Joint Deployment System Functional Description, 24 May 1982.

11. Madnick, Stuart E. and John J. Donovan, Operating Systems, McGraw-Hill Book Company, 1974.

12. Assistant Secretary of Defense (C3I), Modernization of WWMCCS Information System (WIS), 19 January 1981.

13. Evans, Major General Donald L., USAF, WWMCCS Information System Joint Program Office (WIS JPM), speech given to AFCEA-NOVA Chapter, VA, 27 August 1982.

14. Walker, Stephen T., "Department of Defense Data Network", Signal, Volume 37, Number 2, p. 42, October 1982.

15. Factor Comparison Narrative Summary Sheet, DRAFT, For Official Use Only, 23 February 1982, n. pag..

16. Defense Communications Agency, Defense Data Network Program Plan, January 1982, Revised May 1982.

17. Defense Communications Agency and MITRE Corporation, Defense Data Network, Helden, LCOL Heidi B. and Howard C. Duffield, Undated.

18. Joint Deployment Agency, Joint Deployment System Users Manual, 1 March 1982.

19. MITRE Corportation, Users Manual for the Joint Deployment System Remote Users Package (DRAFT), 19 August 1981.

20. Command and Control Technical Center, An Executive Overview of the Joint Operational Planning System, the Crisis Action System, and the Joint Deployment System, June 1980.

21. MITRE Corporation, Joint Deployment System Baseline System Description (WORKING PAPER), 1 Dec 1982.

22. Defense Communications Agency/Command and Control Technical Center, Analysis Report, Results of JCS Worldwide Exercise IVY LEAGUE 82, 25 January 1982, For Official Use Only, 4 October 1982.

23. Cannon, Major Sam, Honeywell DPS Equipment, briefing given at Defense Communications Agency/Command and Control Technical Center, Washington, D.C., April 1982.

24. Fraim, Lester J., SCOMP: A Solution to the MLS Problem, Honeywell Information Systems, 13 August 1982.

25. National Security Agency/DOD Computer Security Center, Product Evaluation Bulletin: SCOMP (Secure Communications Processor), 1 December 1981.

26. Kim, JoAnne, An Approach to Multi-Level Security, unpublished paper for Course Number CO3111, Naval Postgraduate School, December 1981.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	Professor M. G. Sovereign, Code 74 Chairman, C3 Academic Group Naval Postgraduate School Monterey, California 93940	1
4.	LT COL J. W. Johnson, USAF, Code 39 Joint C3 Curricular Officer Naval Postgraduate School Monterey, California 93940	2
5.	CDR Leon B. Garden, USN, Code 62Ge Naval Postgraduate School Monterey, California 93940	1
6.	LT Mary McLendon-Koenig, USN P.O. Box 4162 McLean, Virginia 22103	1
7.	CAPT Gene A. Steffanetta, USMC 10618 Zion Drive Fairfax, Virginia 22032	1
8.	Director National Security Agency ATTN: Miss Joanne Kim, H44 Fort George G. Meade, Maryland 20755	1
9.	LT Sheila K. McCoy, USN Joint C3 Curricular Office, Code 39 Naval Postgraduate School Monterey, California 93940	1

MEI
8